Manuel d’utilisateur
Desktop ClientV28.0.1.12

Avis et clause de non responsabilité (disclaimer)

Ce manuel a pour seul but d'aider les installateurs et/ou les utilisateurs à installer et à utiliser de manière sûre et efficace le système et/ou le produit et/ou le logiciel qui y est décrit.

Avant d'installer et/ou d'utiliser le système, l'installateur et l'utilisateur doivent lire ce manuel et se familiariser avec toutes les instructions de sécurité et les procédures d'utilisation.

- Le système ne doit pas être utilisé à des fins autres que celles pour lesquelles il a été conçu.
- L'utilisation du logiciel associé au système et/ou au produit, le cas échéant, est soumise aux termes de la licence fournie dans le cadre des documents d'achat.
- Ce manuel décrit la configuration maximale du système avec le nombre maximal de fonctions, y compris les options futures. Par conséquent, toutes les fonctions décrites dans ce manuel peuvent ne pas être disponibles dans la configuration spécifique du système et/ou du produit que vous avez acheté.
- Une utilisation ou une installation incorrecte, ou l'incapacité de l'utilisateur à entretenir le système de manière efficace, dégage le fabricant (et le vendeur) de toute responsabilité en cas de non-conformité, de dommages ou de blessures.
- Le texte, les images et les graphiques de ce manuel sont uniquement destinés à des fins d'illustration et de référence.
- Toutes les données contenues dans ce manuel sont susceptibles d'être modifiées sans préavis.
- Le fabricant ne peut en aucun cas être tenu responsable de tout dommage spécial, direct, indirect, accessoire, consécutif, exemplaire ou punitif (y compris, mais sans s'y limiter, tout dommage résultant d'une interruption d'activité, d'une perte de bénéfices ou de ventes).
- Toutes les illustrations de ce manuel sont fournies à titre de référence uniquement, il peut y avoir des différences entre les illustrations et le produit réel.
- Tous les schémas de câblage sont donnés à titre indicatif uniquement, les images des circuits imprimés sont destinées à illustrer et à mieux faire comprendre le produit et peuvent différer des circuits imprimés réels.

Contenu

1. Aperçu

Rosslare Enterprises Ltd. Le logiciel AxTraxPro Desktop Client est un système de gestion de logiciels basé sur le Web à utiliser avec les panneaux de contrôle d'accès de Rosslare Enterprises Ltd. Le système de contrôle d'accès AxTraxPro est convivial, intuitif et riche en fonctionnalités. AxTraxPro vous permet de configurer les fonctions des portes en fonction des zones et des périodes de temps pour différents types de personnel et pour différentes situations d'alarme. Ce manuel est compatible avec la version V28.0.1.12 du logiciel AxTraxPro.

Types d'utilisateurs

Dans le logiciel AxTraxPro Desktop Client, les utilisateurs sont répartis en quatre catégories. Chaque catégorie a un type d'accès différent au système.

Par défaut, un opérateur a un accès complet au système. Un opérateur peut uniquement visualiser et/ou modifier les composants spécifiques du système qui lui sont donnés. Les opérateurs peuvent également bénéficier d'une immunité en matière d'Antipassback, d'interlock ou de lockdown.

Seul un opérateur spécifique peut gérer et contrôler un lockdown

Les utilisateurs et les visiteurs ne sont autorisés à accéder qu'à certaines zones d'accès. Mais ils peuvent également bénéficier d'une immunité Antipassback et d'une immunité de verrouillage.

2. Champ d'application

Ce document contient les procédures d'utilisation du logiciel Rosslare Enterprises Ltd. le logiciel AxTraxPro Desktop Client à utiliser. Le document comprend les éléments suivants pour l'installation et le fonctionnement normaux, ainsi que les fonctions optionnelles et les procédures d'installation supplémentaires dans les annexes:

Procédures d'installation et d'utilisation normales

- Une liste de la configuration requise pour le logiciel AxTraxPro Desktop Client, voir Configuration requise.
- Fournit la procédure d'installation du logiciel AxTraxPro Desktop Client, voir Installation.
- Indique la structure du logiciel AxTraxPro Desktop Client, voir La rubrique Apprendre à connaître l'interface.
- Fournit la procédure de définition des horaires, voir Définir les horaires.
- Donne la procédure pour configurer un site, voir Configuration d'un site.
- Donne la procédure pour ajouter des groupes, voir Gérer les groupes.
- Fournit la procédure pour ajouter des opérateurs, voir Ajouter des opérateurs.
- Fournit la procédure pour ajouter des utilisateurs, voir Gestion des utilisateurs.
- Fournit la procédure pour ajouter des visiteurs, voir Gestion des visiteurs.
- Fournit la procédure d'intégration des systèmes vidéo, voir Intégration des systèmes vidéo.

- Fournit la procédure de visualisation des niveaux d'accès, voir Configuration des niveaux d'accès.
- Fournit la procédure de création des plans d'état, voir Création des plans d'états.
- Fournit la procédure de visualisation des rapports, voir Visualisation des rapports.
- Fournit la procédure d'affichage de l'écran Guard tour, voir Affichage de l'écran Guard Tour.

Fonctions optionnelles et procédures de paramétrage supplémentaires

- Affiche les opérations de l'administrateur, voir Opérations de l'administrateur.
- Affiche la procédure de configuration d'un réseau, voir Configuration d'un réseau.
- Affiche la procédure de configuration des compteurs d'utilisateurs, voir Configurer les compteurs d'utilisateurs. .
- Affiche la procédure d'actionnement manuel d'une porte, voir, Actionnement manuel de la porte.
- Affiche la procédure d'enregistrement d'un visage, voir Enregistrement d'un visage à partir d'un terminal.
- Montre la procédure d'enregistrement d'une plaque d'immatriculation, voir Enregistrement d'un plaque d'immatriculation.
- Affiche la procédure d'enregistrement d'une empreinte digitale, voir Enregistrement d'une empreinte digiale.
- Pour afficher les options du menu Aide, voir Menu Aide.
- Montre la procédure pour ouvrir un programme dans le pare-feu Windows, voir Ouvrir un programme dans le pare-feu Windows.
- Affiche la procédure pour résoudre un problème avec la connexion WAN, voir Résoudre un problème avec la connexion WAN.

3. Spécifications et exigences

3.1. AxTraxPro Server et Client

Le système AxTraxPro comprend séparément les applications logicielles AxTraxPro Server et AxTraxPro Client.

Installez le serveur AxTraxPro sur l'ordinateur qui contrôle les panneaux de contrôle d'accès et gère la base de données.

L'ordinateur doit être un PC dédié au serveur AxTraxPro sans qu'aucune entité SQL ou tout autre service non-Windows n'existe ou ne soit installé sur le PC.

Il est fortement recommandé que le serveur AxTraxPro soit en ligne 24 heures sur 24.

Installez le logiciel client d'AxTraxPro sur tout PC à partir duquel vous souhaitez accéder au système. Un serveur AxTraxPro peut gérer un nombre illimité de clients AxTraxPro.

AxTraxPro est basé sur une architecture client-serveur standard:

- Seul le serveur se connecte à la base de données ; les clients recueillent les informations du serveur.
- Les panneaux sont connectés au serveur via une communication série (RS-485) ou LAN/WAN.
- Par défaut, le serveur fonctionne comme un service Windows.

3.2. Caractéristiques du système

Général	
Architecture du logiciel	Client - Server
Type de base de données	SQL Server Express 2019
Max. Nombre de cartes/badges	• 30.000 par panneau (AC-215IP, AC-215B, AC-225, AC-425) • 5000 (AC-215x) • 100.000 (AC-825IP)
Nombre maximum de groupes d'accès	Basé sur le nombre maximum d'utilisateurs, 30,000 x nombre de panneaux.
Nombre max. de fuseaux horaires	128 (256 met AC-825IP)
Nombre max. Nombre d'identifiants par utilisateur	16
Nombre maximum de panneaux de contrôle d'accès et d'extensions	1023
Antipassback	• Temporisé • Porte • Global – sur l'ensemble du site
Jours fériés internationaux	Jusqu'à 64 jours fériés

Réseau	Description
Nombre maximal de réseaux	jusque 1023 (dépendent la technologie réseau
Panneaux de contrôle d'accès supportés	• AC-215B, AC-215IP-B • AC-225B, AC-225IP-B • AC-225B, AC-225IP-B MD-IO84B • AC-225B, AC-225IP-B avec MD-D02B • AC-425B, AC-425IP-B • AC-425B, AC-425IP-B avec MD-IO84B • AC-425B, AC-425IP-B avec MD-D04B • AC-825IP avec R805, S-805, D-805, P-805 • Legacy: AC-215, AC-215 (SPV), AC-215IP • Legacy: AC-225, AC-225IP • Legacy: AC-225, AC-225IP avec MD-IO84 • Legacy: AC-225, AC-225IP avec MD-D02 • Legacy: AC-425, AC-425IP • Legacy: AC-425, AC-425IP avec MD-IO84 • Legacy: AC-425, AC-425IP avec MD-D04
Interface de communication pour les panneaux	• Sériel (RS-232/485) • TCP-IP L'AC-825IP n'a que le TCP/IP
Vitesse de communication	9600, 19200, 57600, et 115200 bps

3.3. Caractéristiques du système

3.3.1. Configuration requise pour le serveur et le client AxTraxPro

Système d'exploitation	Windows 8.1, 64-bit Windows 10
PROCESSEUR	Minimum: Intel core i5, 2.4 GHz ou plus rapide Recommandé: Intel core i7, 4 cores ou plus haut, 2.4 GHz ou processeur plus rapide
Mémoire	Minimum: 8 GB RAM Recommandé: 16 GB RAM
Réseau	Carte LAN requise pour la mise en réseau TCP/IP
Espace disque dur	Minimum : 4 Go d'espace libre, SSD fortement recommandé

3.3.2. Microsoft Framework

Vous devez avoir Microsoft .NET Framework 4.0 ou plus récent installé sur votre PC.

4. Installation

Le fichier d'installation d'AxTraxPro se compose des quatre éléments principaux suivants:

- Client AxTraxPro
- SQL Serveur
- Serveur AxTraxPro

Le client AxTraxPro n'est requis que sur l'ordinateur principal ; toutefois, il peut être installé sur plusieurs ordinateurs.

4.1. Téléchargement du fichier d'installation d'AxTraxPro

Installez le logiciel de contrôle d'accès AxTraxPro sur l'ordinateur qui se connecte aux panneaux de contrôle d'accès et gère la base de données.

Pour télécharger le fichier d'installation d'AxTraxPro:

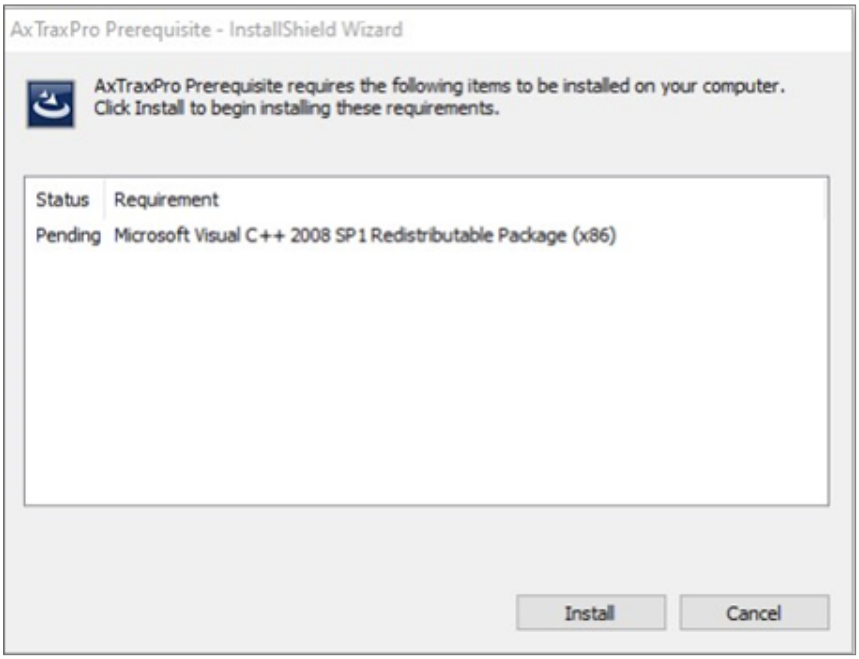
1. Allez sur http://www.rosslaresecurity.com.
2. Connectez-vous à votre compte.
3. Cliquer sur **Download Center** dans la section **Quick Links**.
4. Dans la rubrique **Produit**, sélectionnez la dernière version du logiciel de gestion du contrôle d'accès..
5. Dans Types de **documents**, sélectionnez Logiciels et cliquez sur Rechercher.
   Dans les résultats de la recherche, vous verrez le logiciel **AxTraxPro**
6. Cliquez avec le bouton droit de la souris sur l'icône de téléchargement..
   Le fichier d'installation est téléchargé sur votre ordinateur.

4.2. Démarrer l'installation.

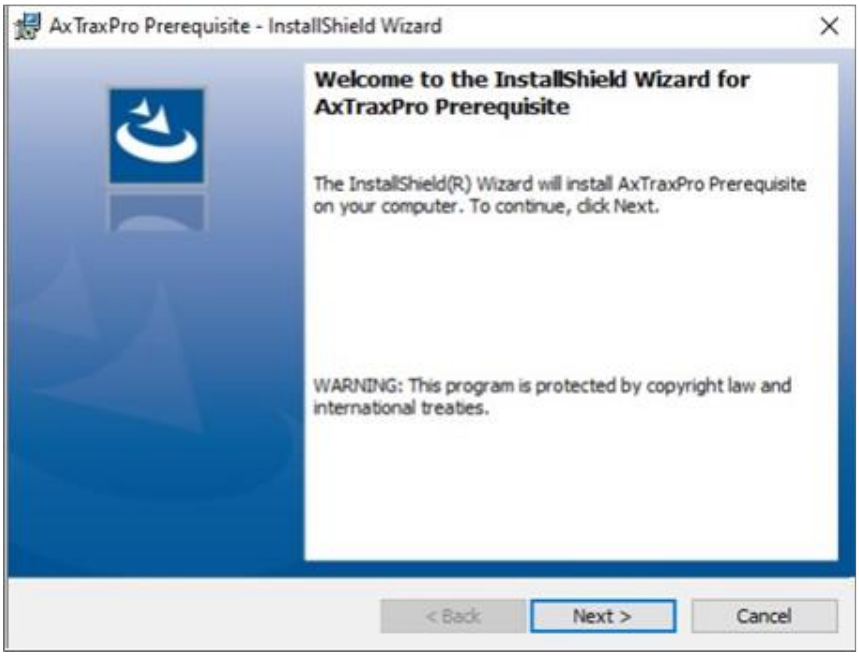
Une fois que vous avez téléchargé le fichier d'installation, vous pouvez commencer l'installation.

Pour démarrer l'installation:

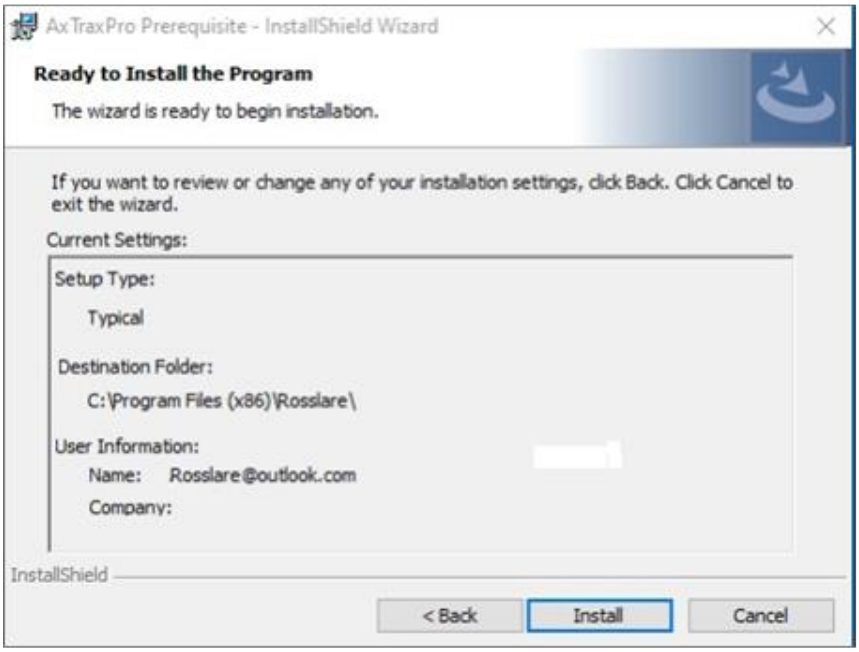
1. Naviguez jusqu'au fichier téléchargé et double-cliquez dessus.
2. Cliquez sur **Installer** une fois que les fichiers requis ont été extraits..



3. Cliquer sur **Next**

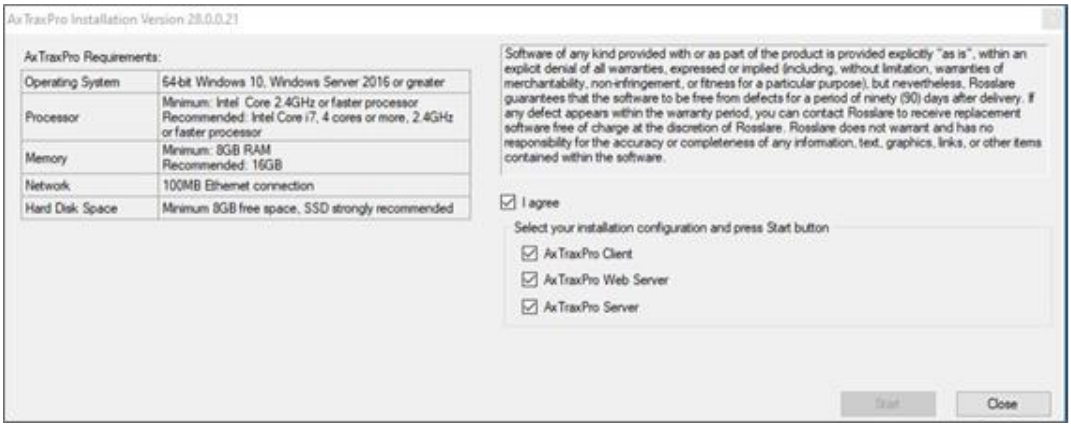


4. Cliquer sur **Install**



5. Cliquer sur **Finish**.

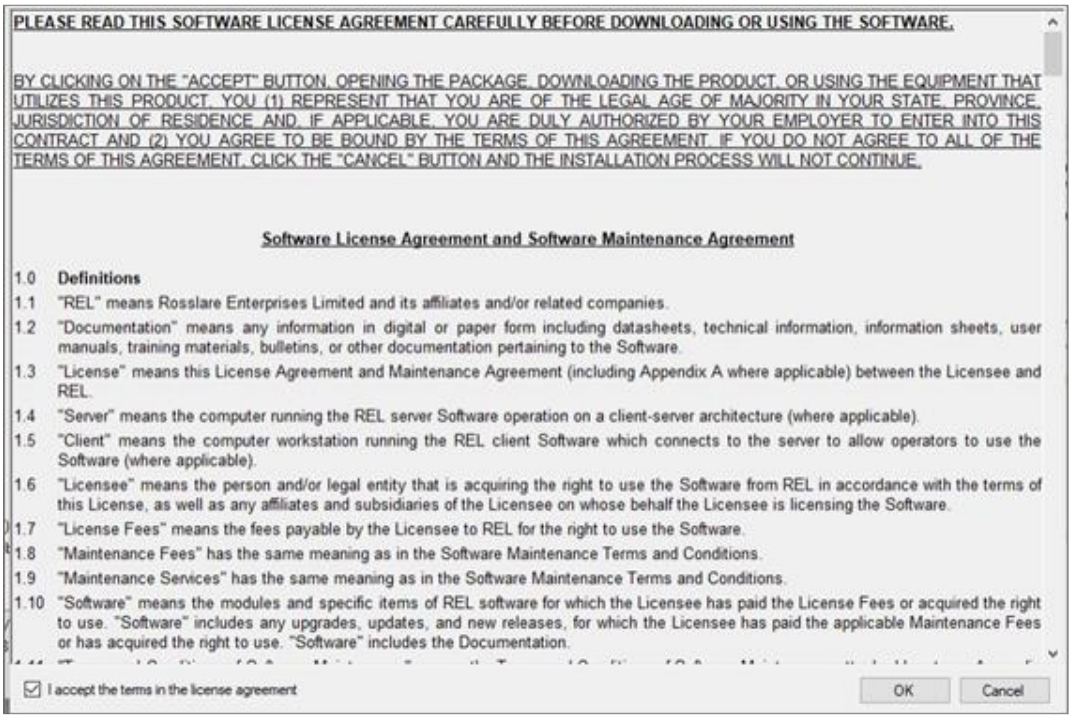
6. Cochez la case "**I Agree**" et choisissez les paquets à installer..



7. Cliquer sur **Start**.

> Cet écran reste ouvert en arrière-plan pendant l'installation des différentes parties du logiciel.

8. Faites descendre la page et lisez l'accord de licence.

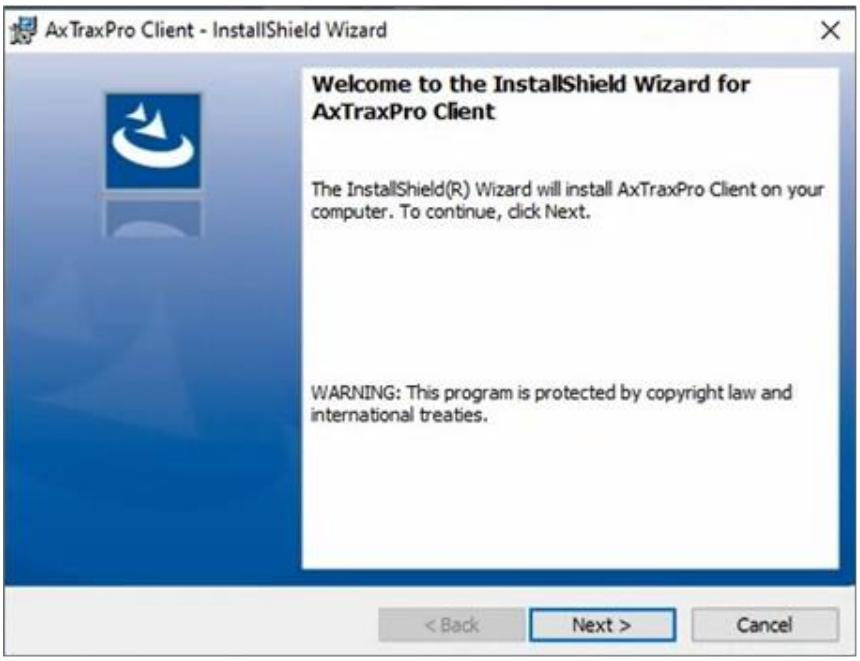


9. Sélectionner "**I accept the terms in the licensing agreement"**.
10. cliquer sur **OK**

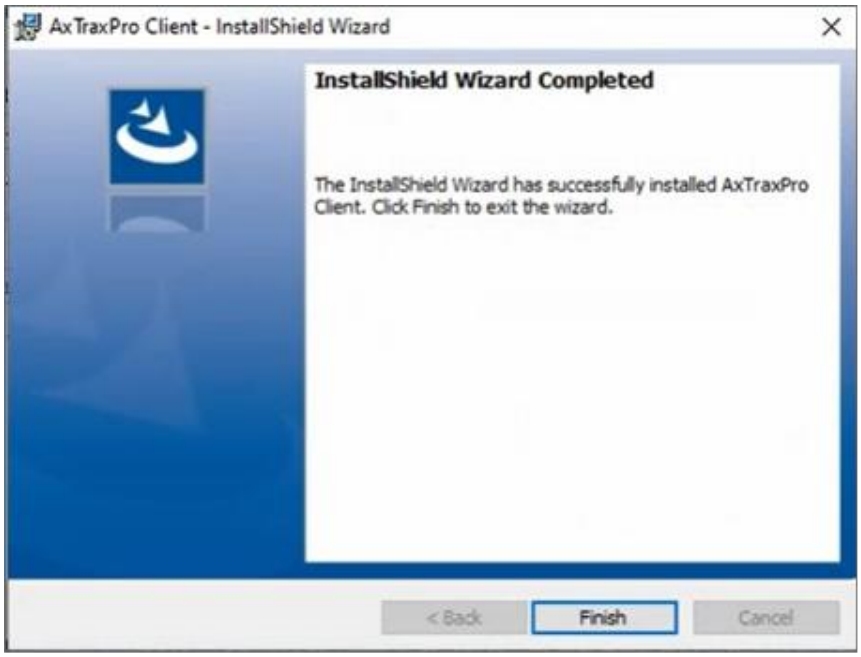
4.3. Installation d'AxTraxPro Client

Pour installer l'application AxTraxPro Client:

1. Cliquer sur “**Next”** pour lancer le processus d'installation de l'application AxTraxPro Client.



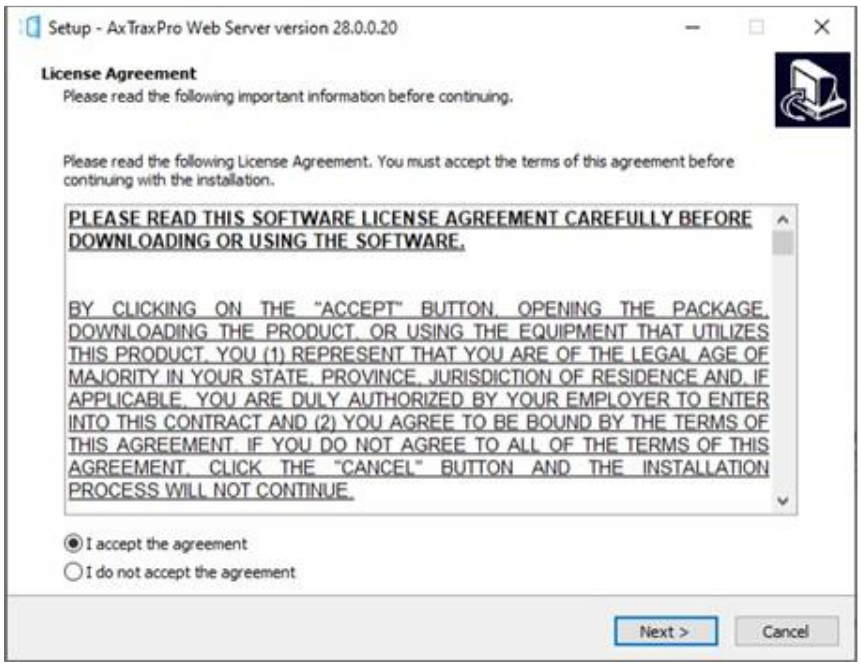
2. Cliquez sur "**Finish**" pour terminer l'installation du client AxTraxPro.



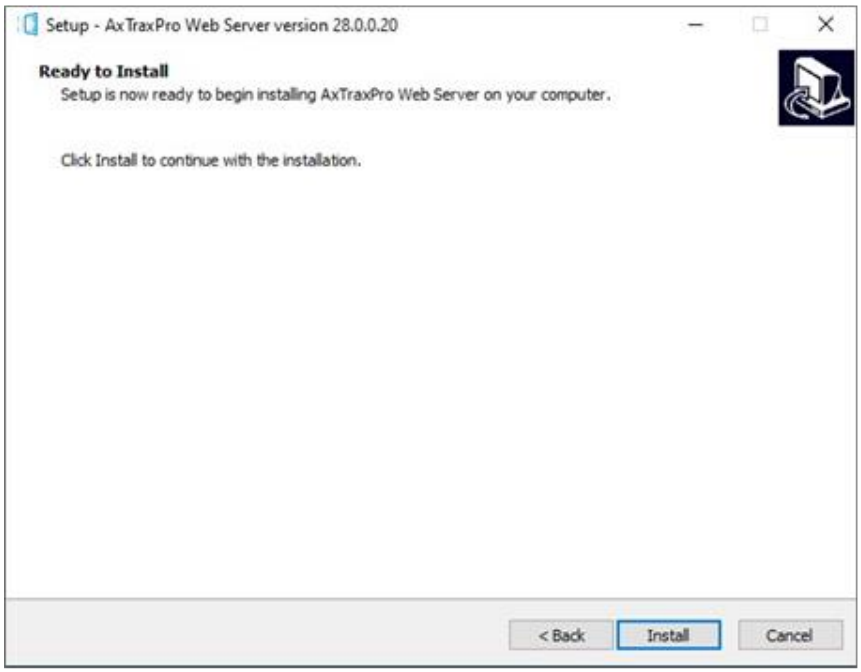
4.4. Installation du serveur Web AxTraxPro

Installation du serveur Web AxTraxPro:

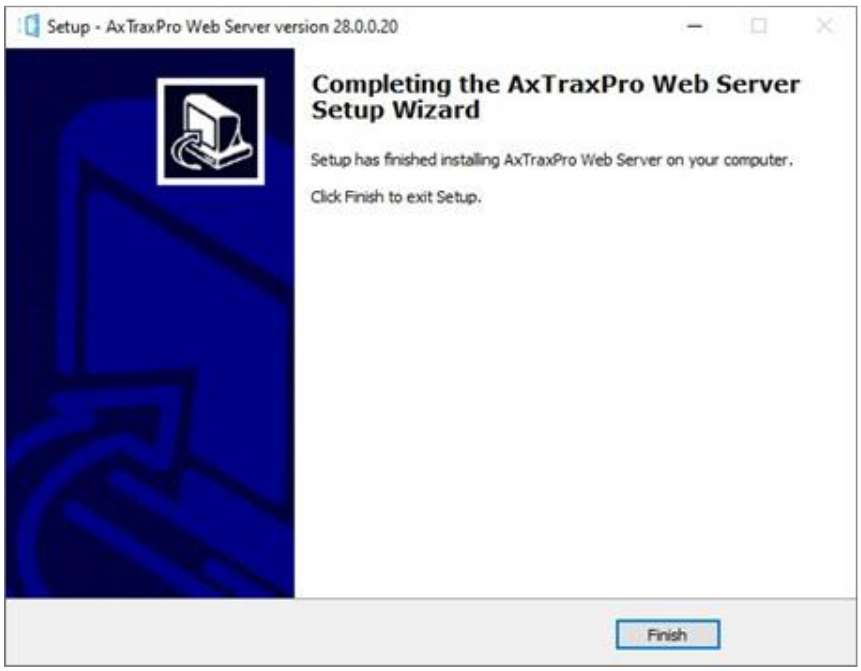
1. Sélectionnez “**I accept the terms in the licensing agreement”** et cliquer sur “**Next”**.



2. Cliquez ensuite sur “**Install”**.



3. Cliquer sur “**Finish**”.

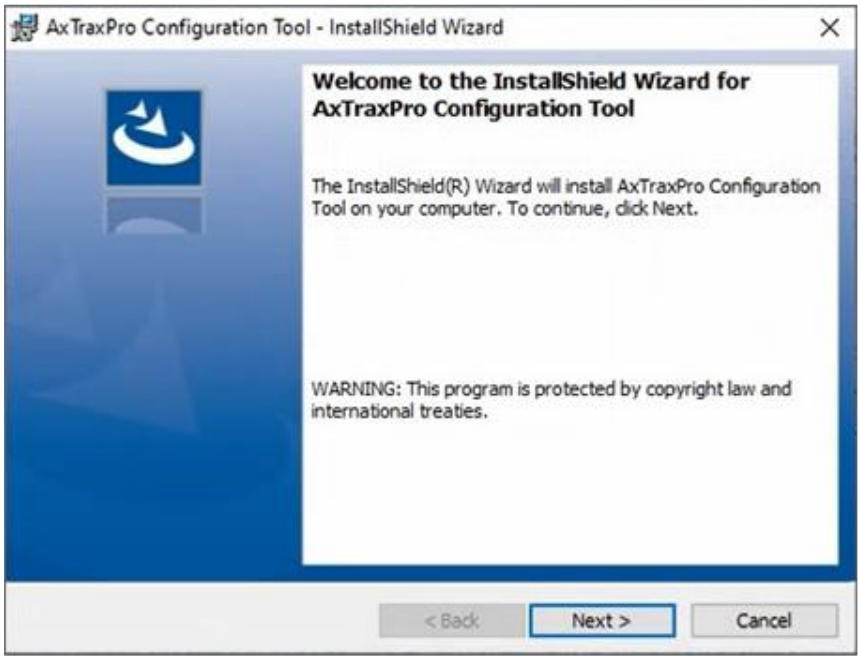


4.5. Outil de configuration d'AxTraxPro

Après avoir installé AxTraxPro Client, une fenêtre s'ouvre pour installer l'outil de configuration d'AxTraxPro.

Pour installer l'outil de configuration d'AxTraxPro:

1. Cliquer sur “**Next**” pour lancer le processus d'installation de l'outil de configuration d'AxTraxPro.



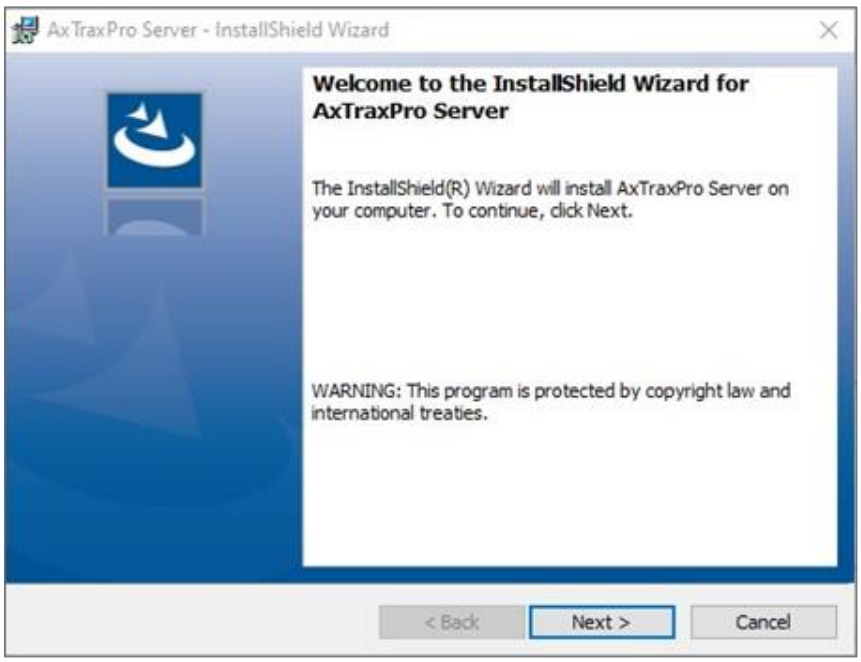
3. Cliquez sur "**Finish**" pour terminer l'installation de l'outil de configuration d'AxTraxPro..

4.6. Installation du logiciel AxTraxPro serveur

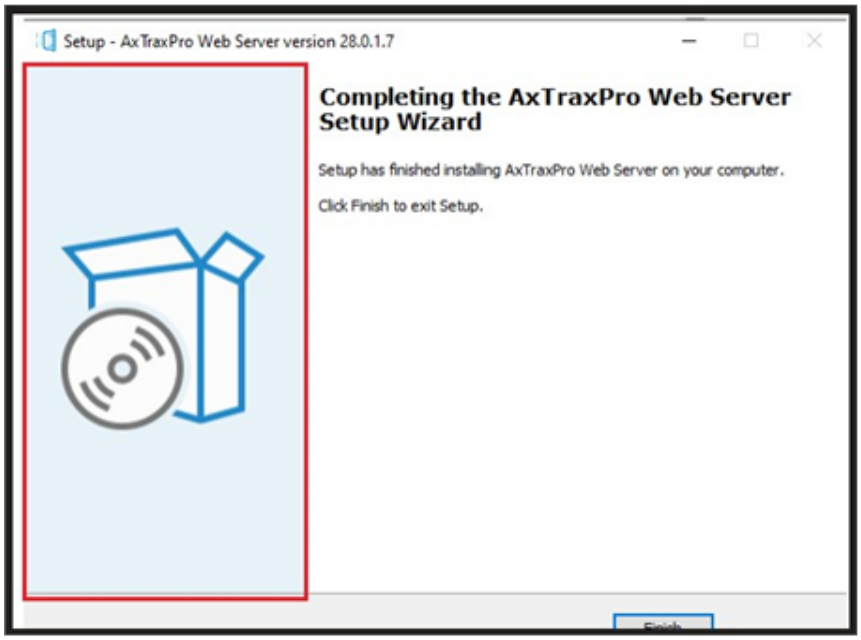
Après avoir installé l'outil de configuration d'AxTraxPro, l'assistant d'installation d'AxTraxPro apparaît pour installer le logiciel du serveur AxTraxPro.

Installation du serveur AxTraxPro:

1. Cliquer sur "**Next"**.



2. Cliquez sur "**Finish**" pour terminer l'installation du serveur AxTraxPro.



4.7. Installation de SQL Serveur

Après avoir installé l'outil de configuration d'AxTraxPro, une fenêtre s'ouvre pour installer le serveur SQL.
Le serveur AxTraxPro fonctionne avec une base de données SQL server 2019. Il y a trois options pour installer le serveur SQL:

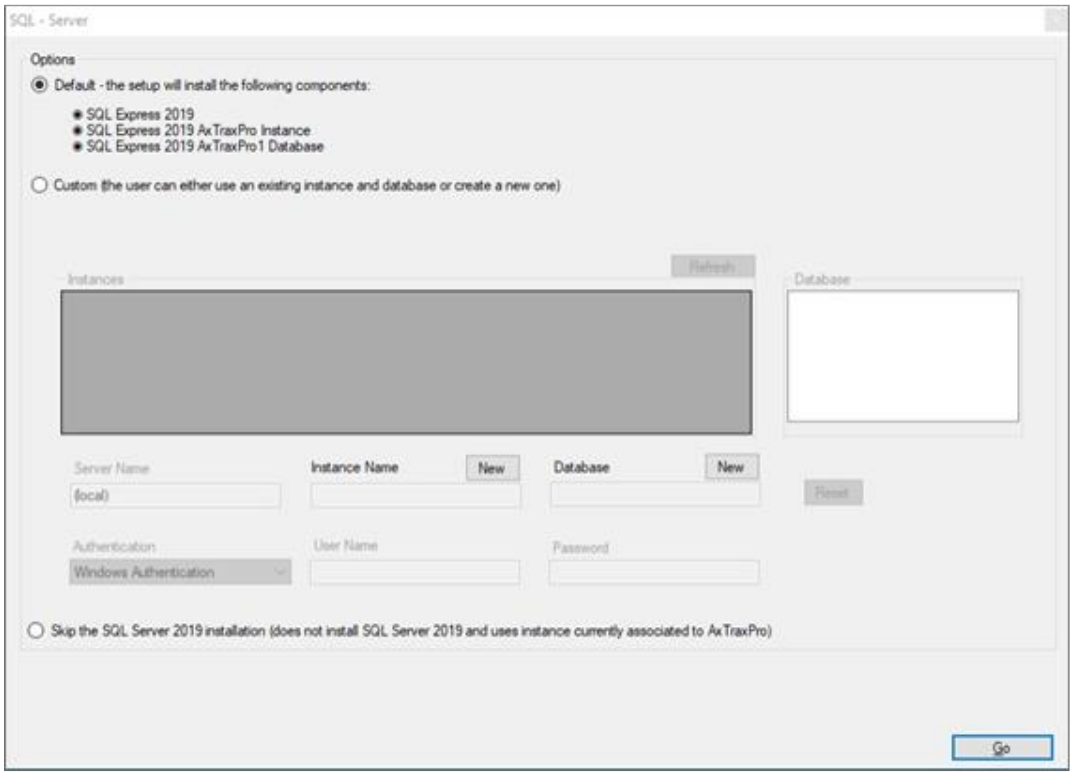
1. Sélectionnez "**Default**" pour installer Microsoft SQL Server Express 2019.
2. Sélectionnez "**Custom**" pour utiliser une instance existante du serveur SQL 2019 disponible sur votre réseau informatique **avec vos identifiants de connexion SQL**.
3. Sélectionnez **"Skip**" pour utiliser l'instance actuelle du serveur SQL d'AxTraxPro..

4.7.1. Installation par défaut

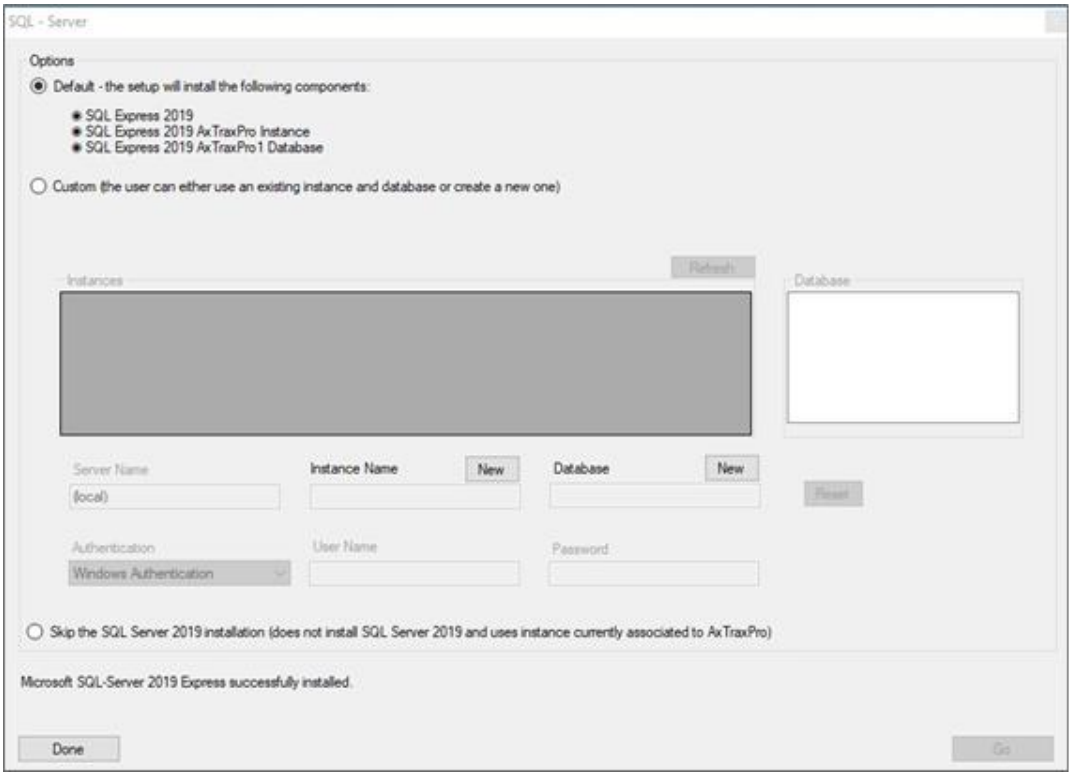
Ne pas installer le serveur SQL lors de l'installation de clients AxTraxPro supplémentaires qui se connectent à la base de données du serveur AxTraxPro.

Pour installer l'application SQL Server standard:

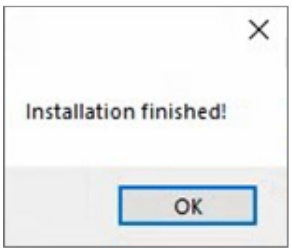
1. Sélectionnez "**Default**" et cliquez sur "**Go**".



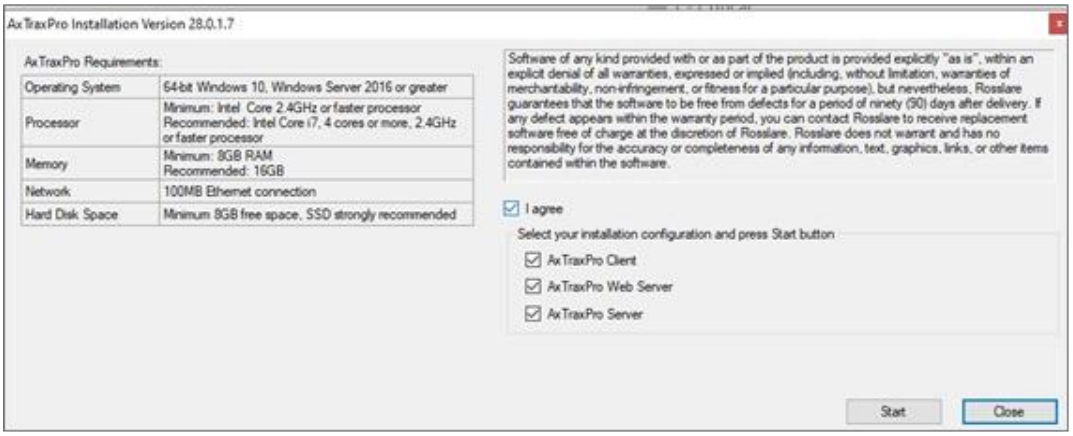
2. Une phrase de confirmation apparaîtra dans la partie inférieure de l'écran lorsque le processus sera terminé. Cliquez sur **"Done**".



3. Cliquer sur **OK**.



4. Cliquer sur **Close**.



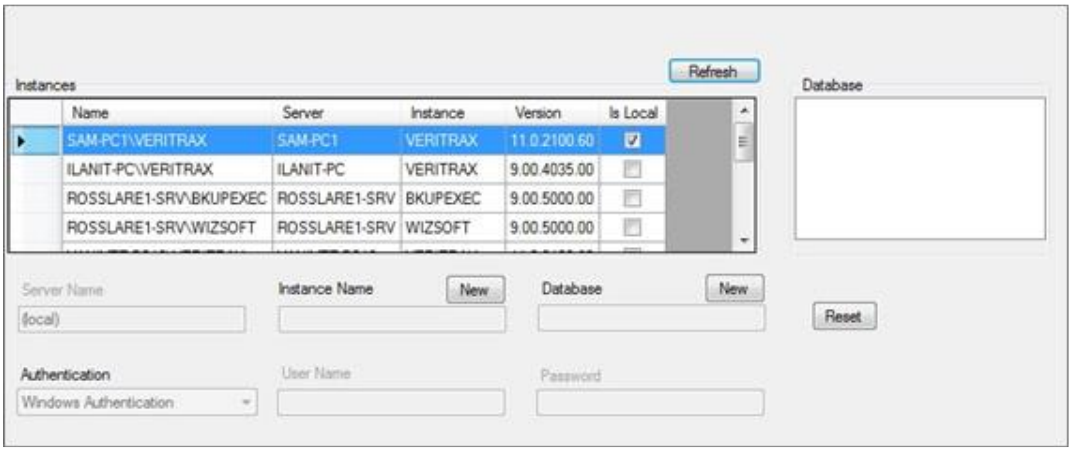
4.7.2. Configuration personnalisée

électionnez "**Custom**" pour utiliser une instance existante du serveur SQL 2019 disponible sur votre réseau informatique avec vos identifiants de connexion SQL:

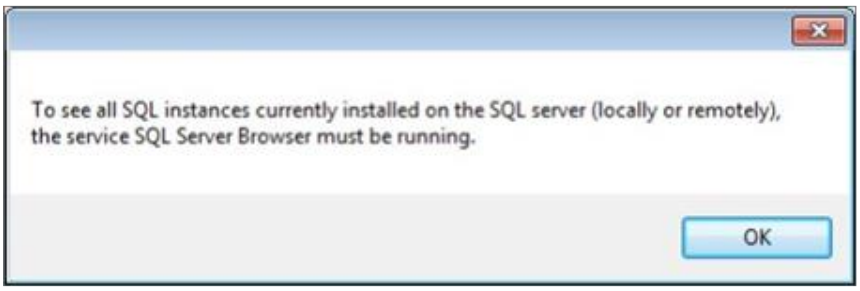
Pour installer une instance existante de l'application SQL Serveur:

1. Sélectionnez “**Custom”**.

   Une liste des instances SQL existantes s'affiche dans le tableau.



Si vous ne voyez pas le tableau, vous obtenez le message suivant à la place:



Vous devez activer et démarrer le service SQL Server Browser, puis cliquer sur "**Refresh"**.

2. Sélectionnez l'instance du tableau que vous voulez utiliser.
3. Saisissez toutes les informations de champ requises.

   Un assistant d'installation pour le SQL Server 2019 Express s'ouvre.

Le mot de passe doit répondre aux exigences du mot de passe fort Microsoft SQL Server:

- Ne contient pas tout ou partie du nom de compte de l'utilisateur
- Est composé de plus de huit caractères
- Contient des caractères d'au moins trois des catégories suivantes
- lettres majuscules anglaises (de A à ZZ)
- Lettres minuscules anglaises (de a à z)
- 10 chiffres de base (0 à 9)
- Caractères non alphabétiques (par exemple !, $, #, %)

- Si une instance de serveur SQL installée dispose de l'authentification SQL Server, il est impossible d'installer une nouvelle instance avec l'authentification Windows.
- Lors de la création d'une nouvelle instance, assurez-vous que le nom de l'instance est différent du nom de l'instance existante.
- La nouvelle instance est créée avec les droits d'administrateur système (utilisateur 'SA'). Pour créer une instance restreinte, demandez à votre administrateur de base de données.

4. Cliquer sur **Go**.

Un assistant d'installation pour SQL Server 2019 Express s'ouvre.

4.7.2.1. Utiliser le serveur SQL actuel

Sélectionnez **Annuler** pour utiliser l'instance actuelle de SQL Server.

Pour utiliser l'instance actuelle de l'application SQL Server:

1. Sélectionnez "**Skip the SQL Server 2019 installation"**.

2. Cliquer sur **Go**.

L'installation continue

4.8. Paramètres du pare-feu

Les paramètres du pare-feu interne peuvent empêcher le serveur AxTraxPro de se connecter à la base de données SQL ou aux contrôleurs de porte via TCP/IP et la connexion serveur-client à distance.

Veuillez contacter votre administrateur système ou le support technique Rosslare pour obtenir des conseils supplémentaires.

4.9. Paramètres du serveur SQL

Après avoir installé AxTraxPro, vérifiez que le service du serveur SQL est en cours d'exécution sur l'ordinateur et qu'il est réglé sur l'installation requise.
Pour plus d'informations sur les paramètres du serveur SQL, voir l'annexe Ouvrir un programme dans le pare-feu de Windows. dans le pare-feu de Windows.

Si SQL Express 2019 est installé (fait partie du paquet d'installation), l'installation doit avoir lieu sur le même compte utilisateur Windows utilisé pour AxTraxPro.

5. Démarrage du logiciel AxTraxPro

AxTraxPro est basé sur la technologie WCF. Une fois AxTraxPro installé sur un PC hôte, le client AxTraxPro est exécuté via une connexion WAN (Internet).

Pour exécuter le client AxTraxPro, vous devez définir les connexions du serveur et du client à l'aide de l'outil de configuration d'AxTraxPro.

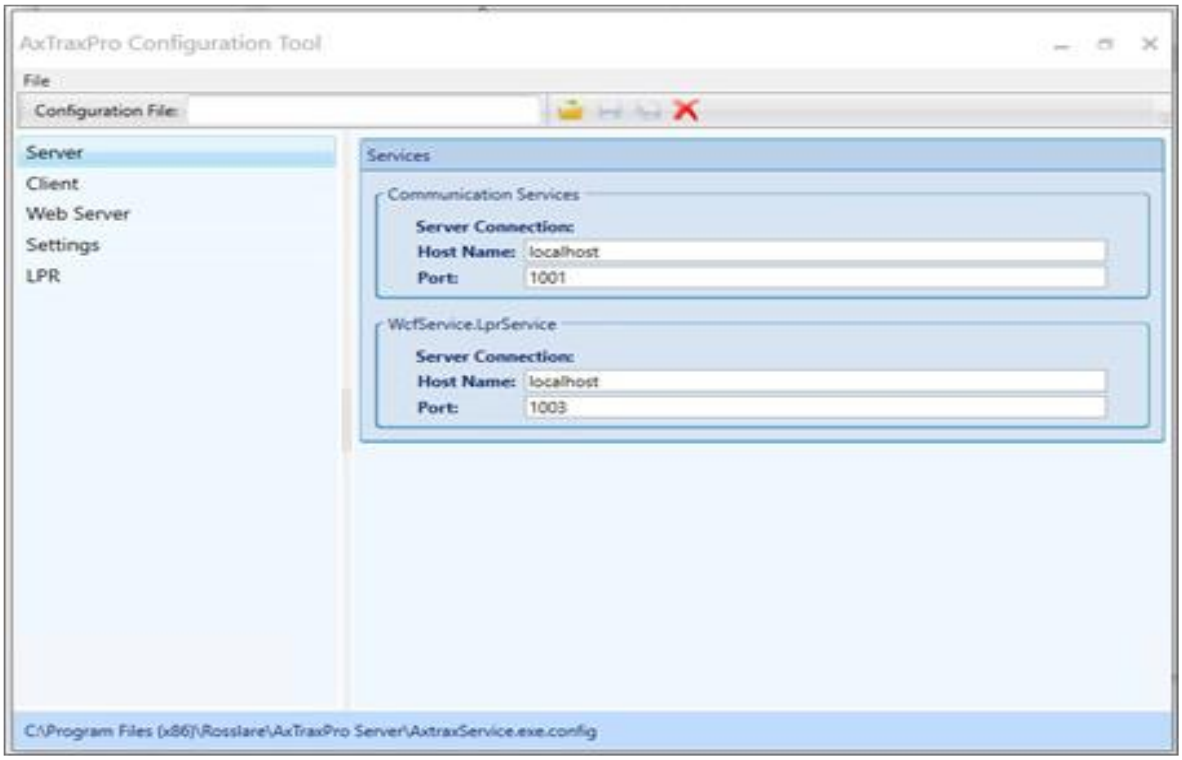
5.1. Configuration de l'hôte AxTraxPro

Pour définir le nom d'hôte du PC hôte d'AxTraxPro:

1. Sur le PC hôte d'AxTraxPro, allez dans **C:\Program Files (x86)\Rosslare\AxTraxPro Configuration Tool**.
2. Exécutez **AxTraxConfigTool** en tant qu'**Administrateur**.
3. Sélectionnez l'onglet **Server**.

4. Dans le champ **Nom d'hôte** de la connexion au serveur de la **section Services de communication**, saisissez l'adresse IP du PC hôte.

5. Cliquer sur **Save**
6. Redémarrez les services AxTraxPro.

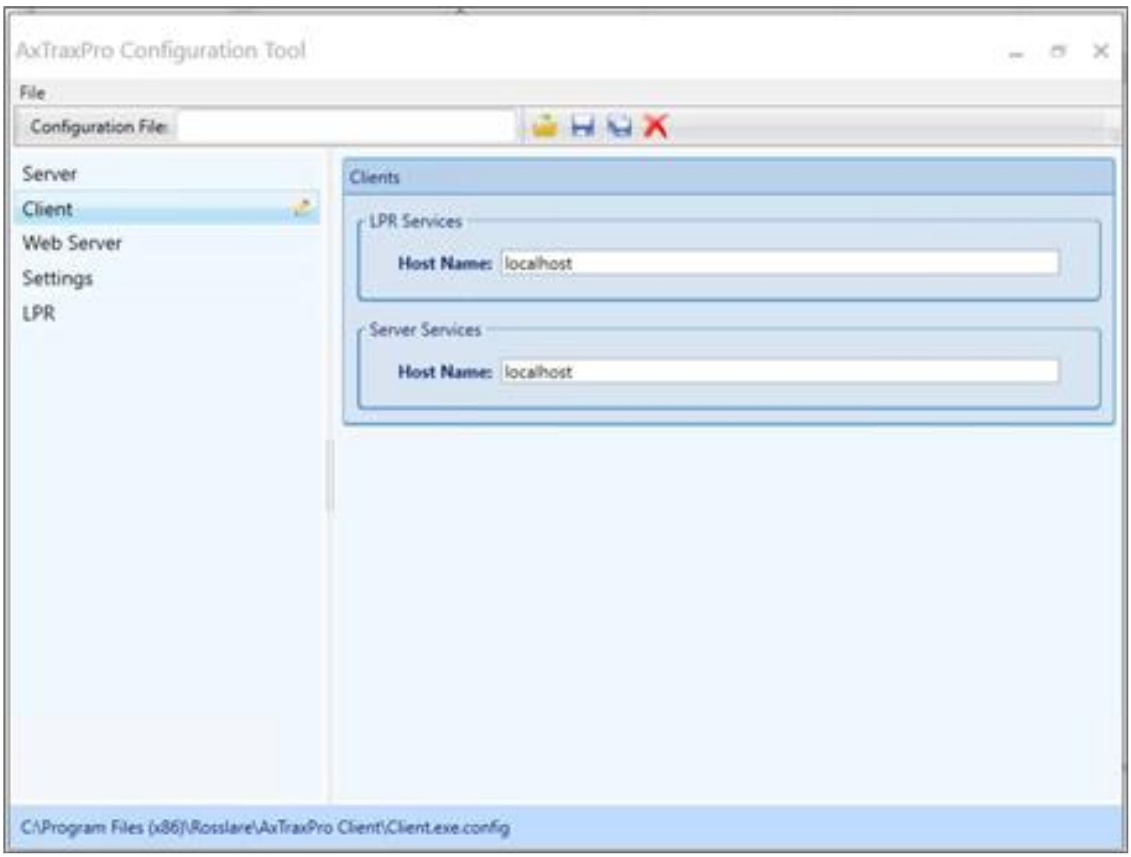


5.2. Configuration de l'AxTraxPro Client

Pour définir le nom d'hôte dans le client PC AxTraxPro:

1. Sur le PC client AxTraxPro, allez dans **C:\Program Files (x86)\Rosslare\AxTraxPro Configuration Tool**.
2. Exécutez l'outil **AxTraxConfigTool** en tant qu'**Administrateur**.
3. Sélectionnez l'onglet **Client.**

4. Dans le champ **Nom de l'hôte** des **Services du serveur**, entrez l'adresse IP du PC hôte.



5. Entrez le numéro de **port.**
6. Cliquer sur **Save**.

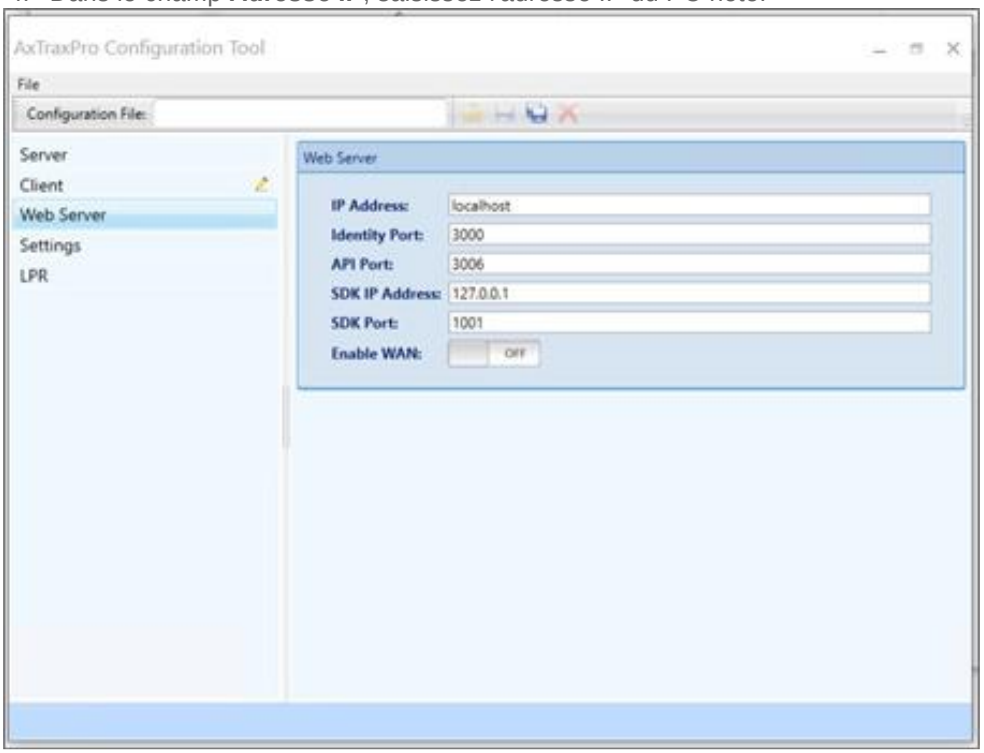
5.3. Configuration du serveur Web d'AxTraxPro

La procédure suivante permet de configurer le serveur web d'AxTraxPro pour qu'il prenne en charge des connexions multiples.

Pour définir l'adresse IP dans le serveur web:

1. Sur le PC client AxTraxPro, allez dans **C:\Program Files (x86)\Rosslare\AxTraxPro Configuration Tool**.
2. Exécutez l'outil **AxTraxConfigTool** en tant qu'**Administrateur**.
3. Sélectionnez l'onglet **Web Server.**

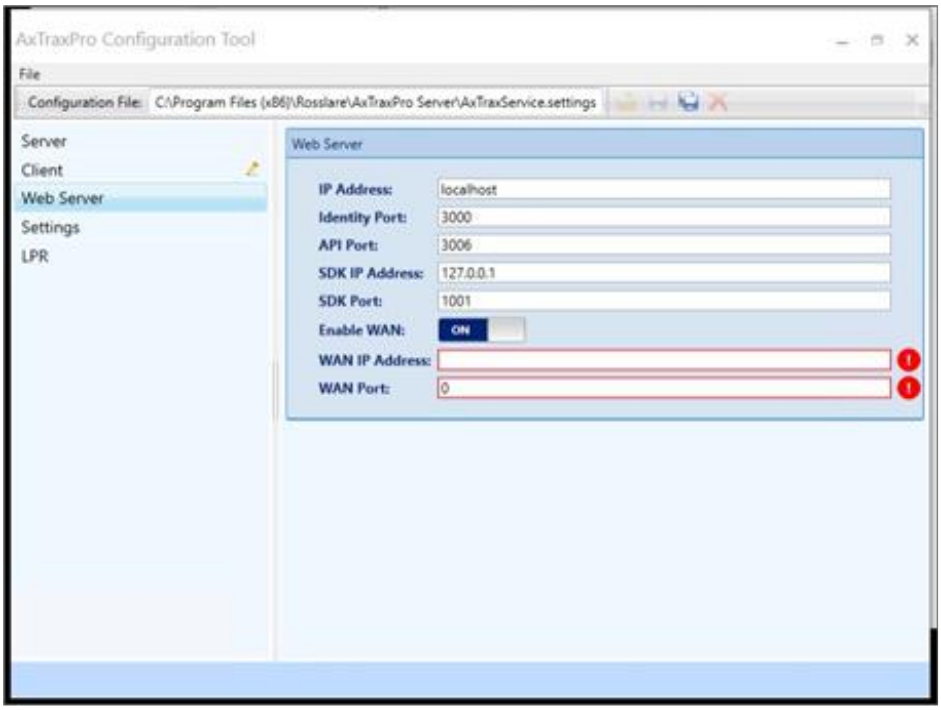
4. Dans le champ **Adresse IP**, saisissez l'adresse IP du PC hôte.



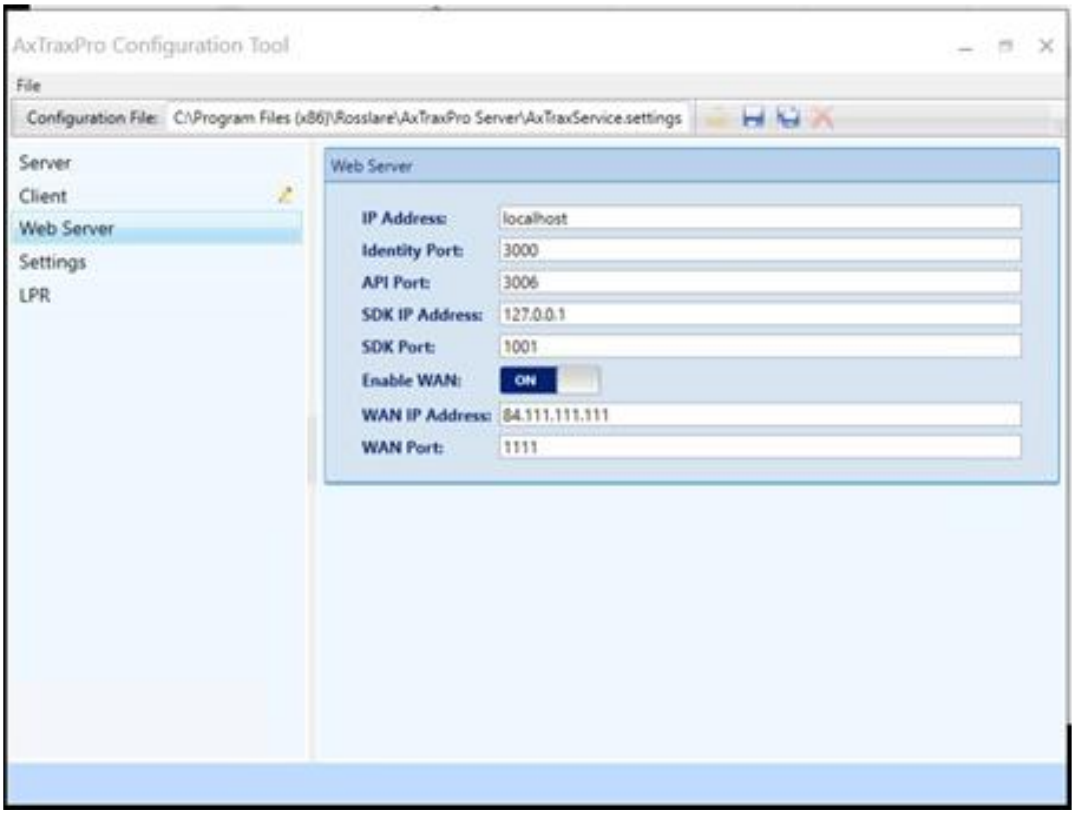
Assurez-vous que le numéro du port d'identité (**Identity Port)** est 3000

Assurez-vous que le numéro du port API (**API Port)**.est 3006.

5. Pour utiliser le serveur Web dans un réseau étendu (WAN), cochez la case.



6. Introduisez les données suivantes:
   a. **WAN IP Address** du routeur public.
   b. **WAN Port** du router.

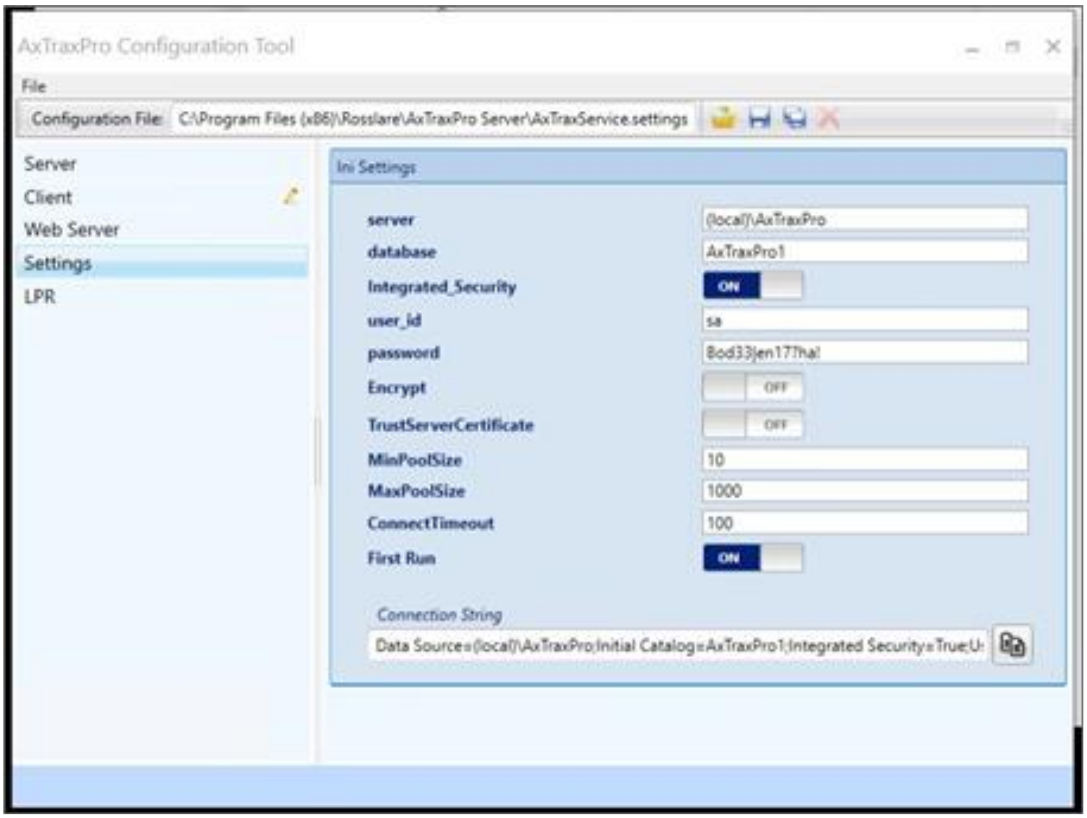


7. Cliquer sur **Save**.

5.4. Paramètres de configuration d'AxTraxPro

Pour configurer l'AxTraxPRO:

1. Sur le PC client AxTraxPro, allez vers **C:\Program Files (x86)\Rosslare\AxTraxPro Configuration Tool**.
2. Exécutez l'outil **AxTraxConfigTool** en tant qu'**Administrateur**.
3. Sélectionnez l'onglet **"Settings".**



4. Insérez le nom du **serveur**.
5. Insérez le nom de la base de données (**database)**.
6. Pour utiliser la sécurité intégrée, sélectionnez le bouton **Integrated_Security**.
7. Entrez le **user_id**.
8. Introduisez le **mot de passe**.
9. Pour utiliser le cryptage, sélectionnez le bouton **Encrypt**
10. Pour accepter le certificat de serveur, sélectionnez le bouton **TrustServerCertificate**.
11. Entrez une taille de pool minimale (**MinPoolSize).**
12. Entrez une taille de pool maximale (**MaxPoolSiz**).
13. Entrez un **ConnectTimeout**.
14. Pour utiliser First Run, sélectionnez l'option du bouton **First Run**.
15. Entrez une chaîne de connexion (**Connection String**).
16. Cliquer sur **Save**

5.5. Démarrer le logiciel AxTraxPro

Cette section explique comment démarrer le système de contrôle d'accès AxTraxPro et comment se connecter.

Pour démarrer le logiciel AxTraxPro:

1. Double-cliquez sur l'icône AxTraxPro client sur le bureau ou sélectionnez le programme dans le dossier Rosslare Enterprises Ltd. Dans le menu Démarrer.

2. Introduisez un nom d'opérateur (**Operator name**).

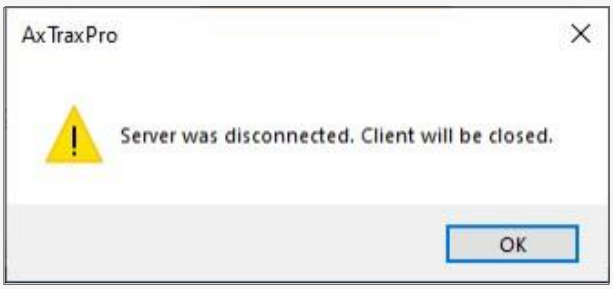
> Le nom par défaut de l'opérateur est administrateur (**administrator)**.

3. Introduisez un mot de passe (**Password)**.

> Le mot de passe (**Password) par défaut** est **admin**.

4. Cliquer sur **OK**.

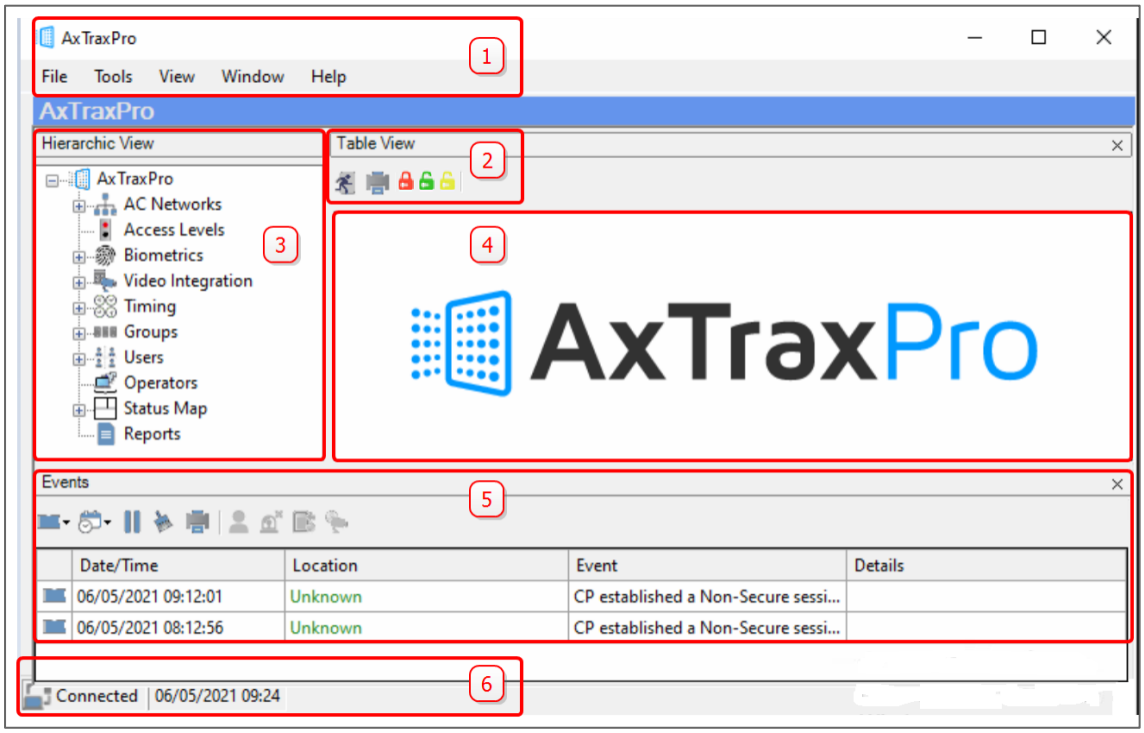
Si la connexion au serveur AxTraxPro est perdue, l'image suivante s'affiche. Pour se connecter au serveur AxTraxPro, voir Configuring the AxTraxPro web server.



6. Découvrir l'interface

Le Rosslare AxTraxPro client est une interface de navigateur web permettant de gérer les panneaux de contrôle d'accès de Rosslare Enterprises Ltd.

L'image et le tableau suivants décrivent la fenêtre principale de Rosslare AxTraxPro.



#	Item	Description
1	Barre de menu	La barre de menu permet de contrôler le fonctionnement général et le paramétrage du logiciel.
2	Barre d'outils	La barre d'outils principale est composée d'icônes pour les tâches les plus importantes lors de la gestion du contrôle d'accès dans un organisme. Les icônes disponibles changent en fonction de la vue sélectionnée. Les touches Lockdown  sont disponible dans toutes les veus de tableau, voir **Utilisation des groupes Lockdown** pour les différents fonctionnements des groupes Lockdown.
3	Vue hiérarchique	La vue hiérarchique ou arborescence permet aux utilisateurs de configurer, surveiller et contrôler tous les aspects du contrôle d'accès.
4	Zone d'affichage	La zone de visualisation affiche tous les éléments de l'élément d'arborescence sélectionné. Elle offre également des options permettant d'ajouter, de modifier ou de supprimer* manuellement des éléments sans ouvrir les fenêtres détaillées des éléments. En outre, la zone d'affichage fournit diverses mises à jour du système.
5	Journal des événements	Le journal des événements affiche un journal détaillé de chaque fois que l'accès a été accordé ou refusé pour chaque porte du site, ainsi que des moments où les entrées et les sorties ont été ouvertes ou fermées. La barre d'outils du journal des événements est composée d'icônes qui permettent à l'utilisateur de surveiller les éventuelles tentatives de sabotage ou d'effraction des portes. Ces alertes sont enregistrées et affichées comme des alertes système internes.
6	Barre d'état	La barre d'état indique l'état de la connexion au serveur et l'heure du serveur.

* Pour supprimer un élément, sélectionnez-le dans la zone d'affichage et cliquez sur l'icône dans la barre d'outils. La touche **Supprimer** du clavier n'est pas prise en charge pour tous les éléments.

7. Définir les délais

Le logiciel AxTraxPro peut gérer un système de contrôle d'accès situé dans une zone géographique différente de celle du serveur. Des plages horaires peuvent être spécifiées pour le système.

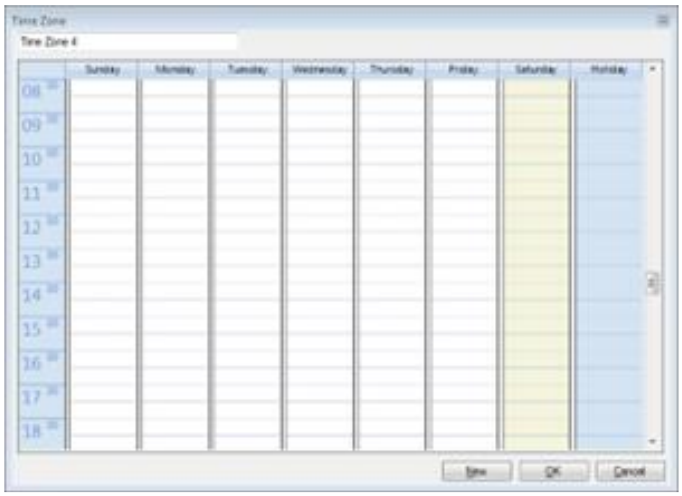
7.1. Ajouter des fuseaux horaires

Un fuseau horaire est un groupe de périodes dans une semaine. Les droits d'accès aux portes, les alarmes et les comportements d'entrée et de sortie peuvent tous être configurés pour se comporter différemment pour chaque fuseau horaire. De nombreuses actions peuvent être automatiquement activées ou désactivées dans un fuseau horaire donné.

La fenêtre des propriétés du fuseau horaire montre les **périodes sélectionnées** pour chaque jour de la semaine..

Pour ajouter un nouveau fuseau horaire:

1. Dans l'arborescence, sélectionnez **Timing > Timezone**.
2. Dans la barre d'outils, cliquez sur l'icône 



3. Entrez un nom pour le fuseau horaire.
4. Cliquez et faites glisser la souris sur une colonne de jours pour sélectionner un intervalle de temps.
5. Cliquez avec le bouton droit de la souris sur la zone sélectionnée et sélectionnez **Créer.**
6. Cliquez à nouveau avec le bouton droit de la souris sur la zone sélectionnée et sélectionnez **Propriétés** pour affiner l'intervalle de temps, puis cliquez sur **OK**.
7. Répétez les étapes 4 à 6 pour chaque jour.

> Un maximum de 16 intervalles peut être ajouté par jour

8. Cliquez sur **OK** lorsque tous les fuseaux horaires sont définis..

> Le panneau de commande AC-215A peut prendre en charge jusqu'à 8 intervalles de temps pour chaque jour.

7.2. Ajouter des jours fériés

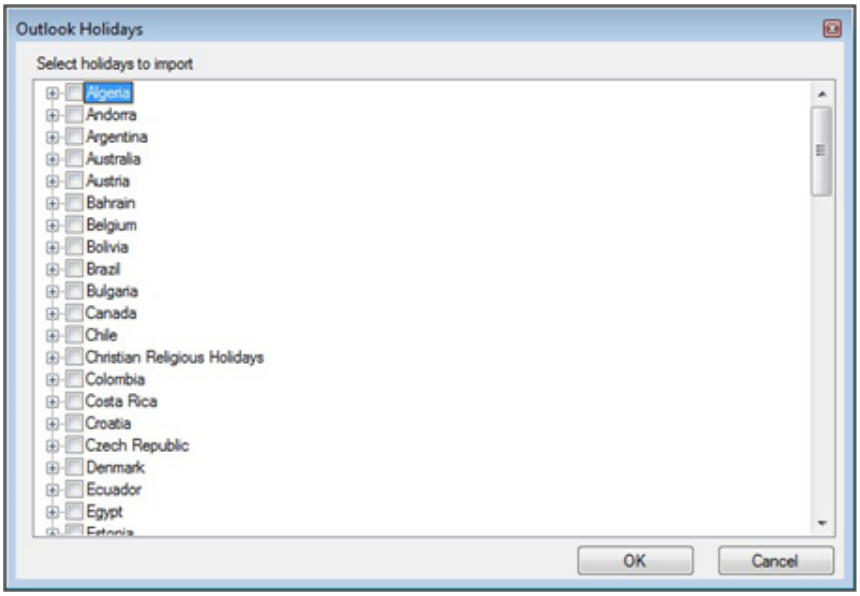
Vous pouvez ajouter et définir des dates de vacances annuelles pour lesquelles il est ensuite possible de définir un statut d'accès spécial.

Il y a deux façons d'ajouter des jours fériés:

- Ajouter un ou plusieurs jours fériés nationaux connus.
- Ajouter un nouveau jour férié.

Pour ajouter un jour férié:

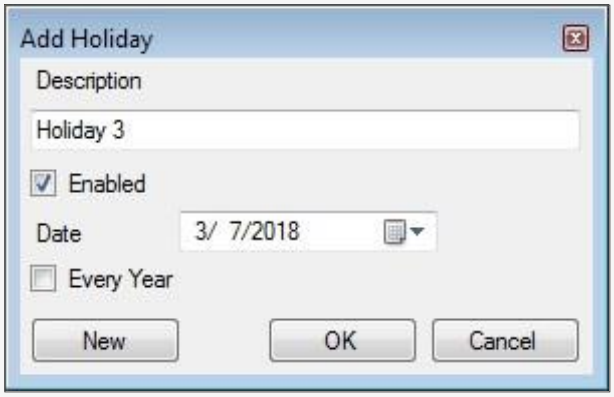
1. Dans l'arborescence, sélectionnez **Timing > Jours fériés.**
2. Dans la barre d'outils, cliquez sur l'icône 



3. Trouvez le pays concerné dans la liste et sélectionnez:
   a. Cochez la case principale pour sélectionner tous les jours fériés de ce pays.
   b. Développez la case à cocher et sélectionnez les jours fériés que vous souhaitez ajouter.
4. Cliquer sur **OK**.

Pour ajouter un nouveau jour férié :

1. Dans l'arborescence, sélectionnez **Timing > Jour férié**
2. Dans la barre d'outils, cliquez sur l'icône 



3. Dans **Description**, saisissez le nom du jour férié..
4. Sélectionnez **Activer** pour activer le jour férié.
5. Utilisez le menu déroulant **Date** pour sélectionner le ou les jours fériés..
6. Cochez **Chaque année** pour que le jour se reproduise chaque année.
7. Cliquer sur **OK**.

8. Configuration d'un site

Le site de contrôle d'accès comprend un ou plusieurs réseaux de contrôle d'accès. Le PC AxTraxPro client communique avec chaque panneau de contrôle d'accès dans le réseau.

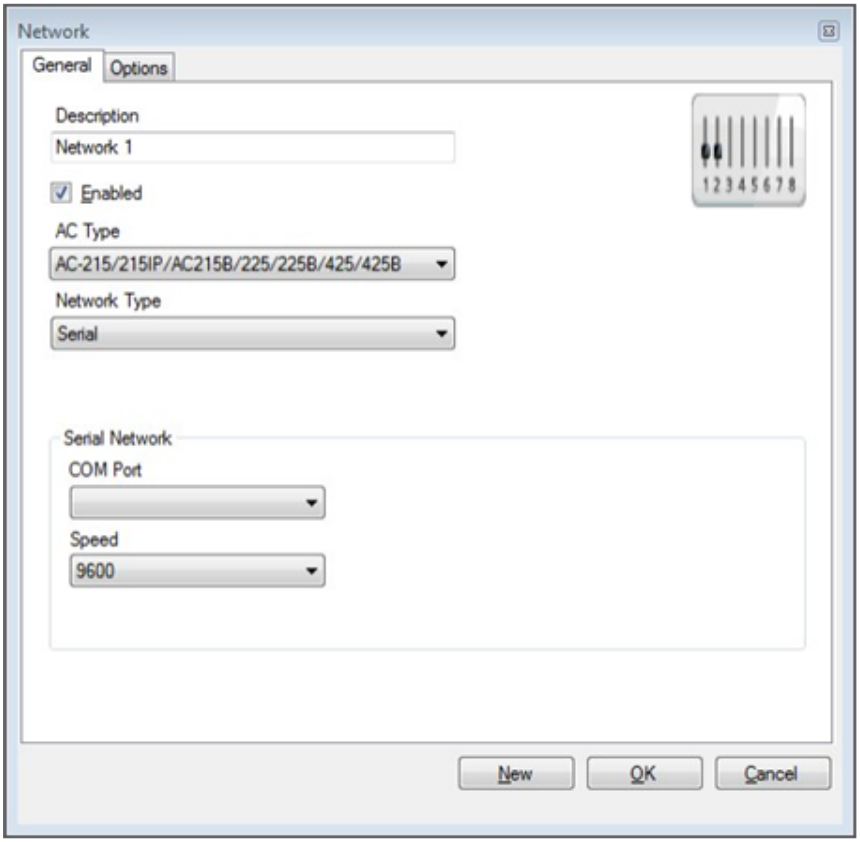
Lorsque vous ajoutez un réseau, vous devez sélectionner le type de panneaux de contrôle d'accès dans le réseau.

8.1. Ajouter un réseau pour les panneaux AC-215x, AC-225x et AC-425x

Pour ajouter un réseau pour les panneaux AC-215x, AC-225x et AC-425x:

1. Dans l'arborescence, sélectionnez **AC Networks**.

2. Dans la barre d'outils, cliquez sur l'icône 



3. Dans **Description**, saisissez un nom pour le réseau.

4. Cochez "**Enabled"**.

> Si "**Enabled"** n'est pas coché, la communication avec les panneaux est arrêtée.

5. Dans **AC Type**, sélectionnez **AC-215/215IP/215B/225/225B/425/425B**.

6. Dans **Network Type**, sélectionnez le type de réseau et définissez les paramètres de connexion:
   a. Sélectionnez le port COM et la vitesse appropriés pour Sériel.
   b. Pour un réseau TCP/IP, entrez l'adresse IP, sélectionnez le port et la vitesse. Sélectionnez également s'il s'agit d'un réseau WAN ou LAN.

7. Si vous ne connaissez pas les paramètres de connexion:
   a. Pour une connexion TCP/IP, cliquez sur **Configurer** pour localiser le hardware sur le réseau local. .

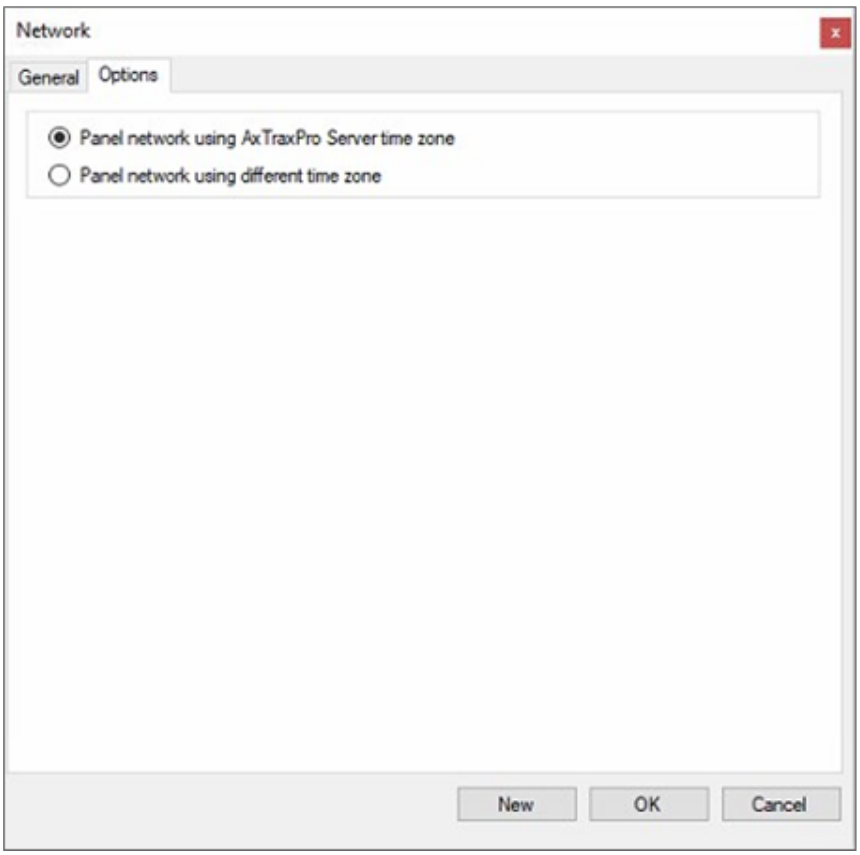
   Voir Configuration d'un réseau pour la procédure de configuration d'un réseau de contrôle d'accès. Consultez votre administrateur système pour plus d'informations ou contactez le support technique Rosslare.

   Les panneaux de contrôle d'accès se connectent à un réseau TCP/IP via une passerelle MD-N32 Serial to Ethernet ou via le module intégré dans l'AC-225IP ou l'AC-425IP. Référez-vous aux guides d'installation des matériels concernés pour plus de détails.

8. Pour tous les types de réseaux, configurez le commutateur DIP sur le matériel du panneau de contrôle d'accès selon le diagramme en haut de l'écran.

   Après avoir modifié le commutateur DIP, éteignez puis rallumez les panneaux.

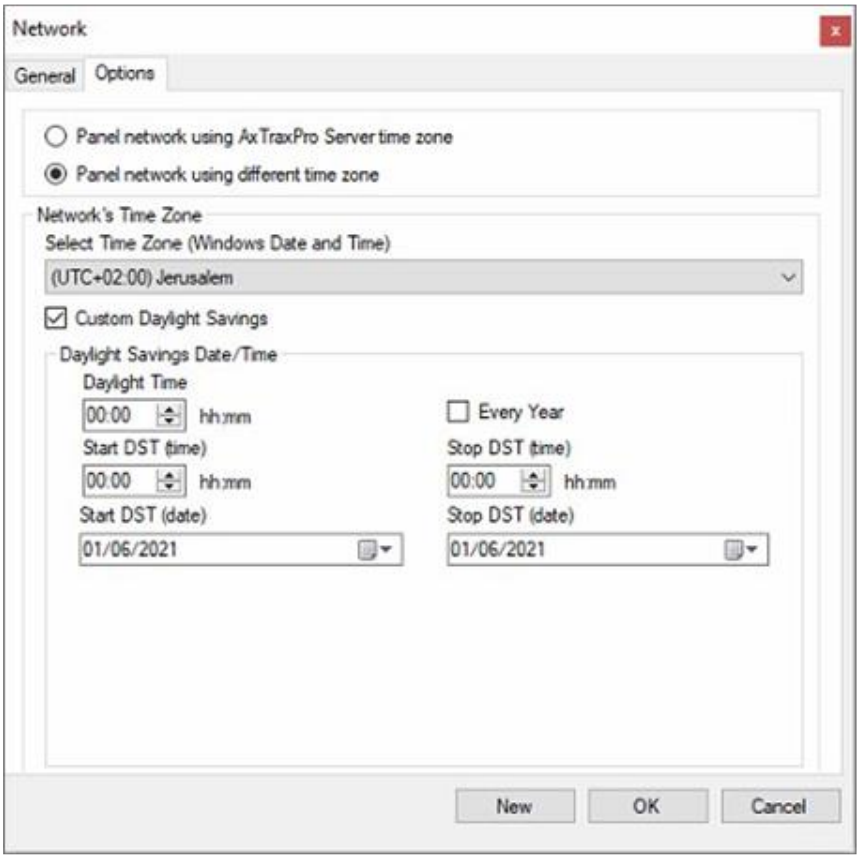
9. Dans la fenêtre **Réseau**, sélectionnez l'onglet **Options**..



10. Pour utiliser le fuseau horaire du serveur AxTraxPro pour le réseau de panneaux, sélectionnez **Panel Network with AxTraxPro Server time zone** (default) (Réseau de panneaux avec fuseau horaire du serveur AxTraxPro) et passez à l'étape 13.

11. Pour sélectionner un fuseau horaire différent pour le réseau de panneaux, sélectionnez Réseau de **panneaux avec un fuseau horaire différent.**

12. Cochez la case **Personnaliser l'heure d'été**



13. Définissez les définitions de l'heure d'été selon les descriptions des champs du tableau suivant..

Champs	Description
Daylight saving time (heure d'été)	Sélectionnez la nouvelle heure à laquelle l'heure d'été commence.
Démarrer DST (temps)	Sélectionnez l'heure à laquelle l'heure d'été commence.
Arrêter DST (temps)	Sélectionnez l'heure à laquelle l'heure d'été se termine.
Chaque année	Sélectionnez **Chaque année** pour définir un jour dans l'une des semaines d'un mois défini pour démarrer et terminer automatiquement l'heure d'été chaque année. Effacer **Chaque année** pour définir une date de début et de fin de l'heure d'été une fois. Dans ce cas, une nouvelle date doit être définie chaque année.
Démarrer DST (temps)	Si l'option **Chaque année** n'est pas sélectionnée, sélectionnez la date de début de l'heure d'été
Arrêter DST (temps)	Si **Chaque année** n'est pas sélectionné, sélectionnez la date de fin de l'heure d'été.

14. Pour enregistrer ce réseau/panneau et ajouter un autre panneau, cliquez sur **Nouveau.**

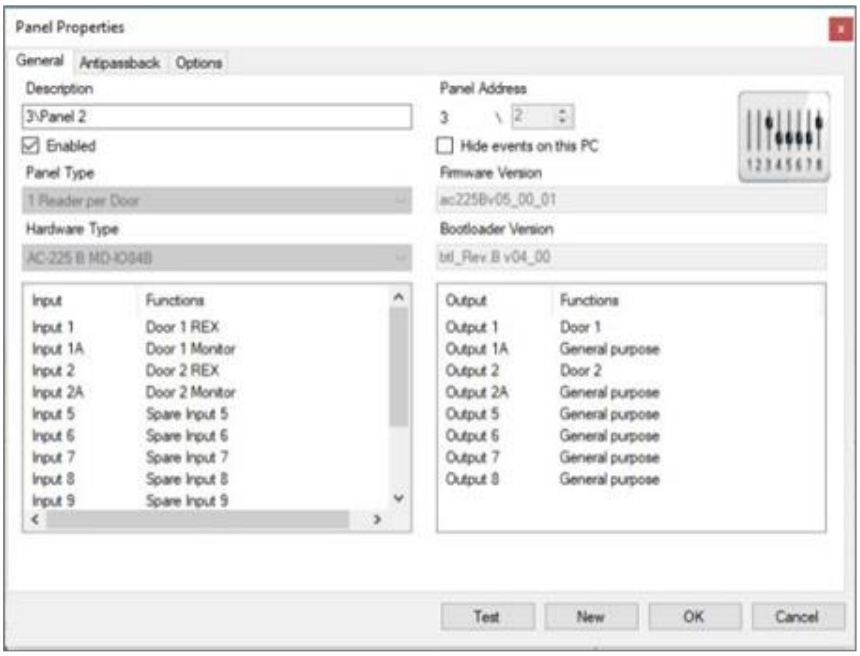
15. Pour enregistrer ce réseau/panneau et fermer la fenêtre, cliquez sur **OK**.

8.2. Ajouter un panneau de contrôle d'accès à un réseau existant

Vous pouvez ajouter un panneau individuel en utilisant **l'arborescence**.

Pour ajouter un panneau individuel:

1. Dans l'**arborescence**, cliquez sur **AC Networks**.
2. Sélectionnez un réseau disponible.
3. Dans la barre d'outils, cliquez sur l'icône 



4. Pour ajouter le panneau et le configurer à un autre moment, sélectionnez **OK**
5. Pour ajouter et configurer le panneau, sélectionnez **Nouveau** (voir Configuration d'un panneau pour la procédure de configuration du panneau).

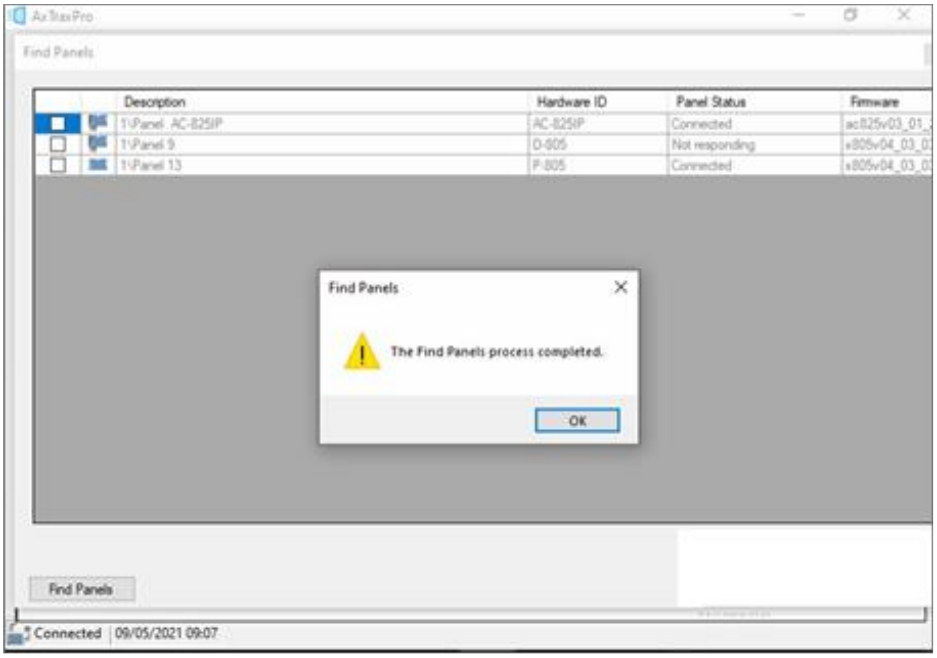
8.3. Chercher des panneaux de contrôle d'accès existants

l est possible de chercher des panneaux dans le réseau de contrôle d'accès en utilisant l'option **Chercher des panneaux**. AxTraxPro trouve tous les panneaux connectés dans le réseau et les vérifie. Les panneaux peuvent alors être rapidement activés et mis à jour.

Pour chercher un panneau existant dans le réseau:

1. Dans l'arborescence, développez l'élément **Réseaux AC** et sélectionnez un réseau..

2. Dans la barre d'outils, cliquez sur l'icône 



Une fois le processus de détection terminé (cela peut prendre plusieurs minutes), l'écran affiche tous les panneaux détectés et les informations qui leur sont associées.

3. Sélectionnez les panneaux que vous souhaitez ajouter et cliquez sur **Ajouter des panneaux**.

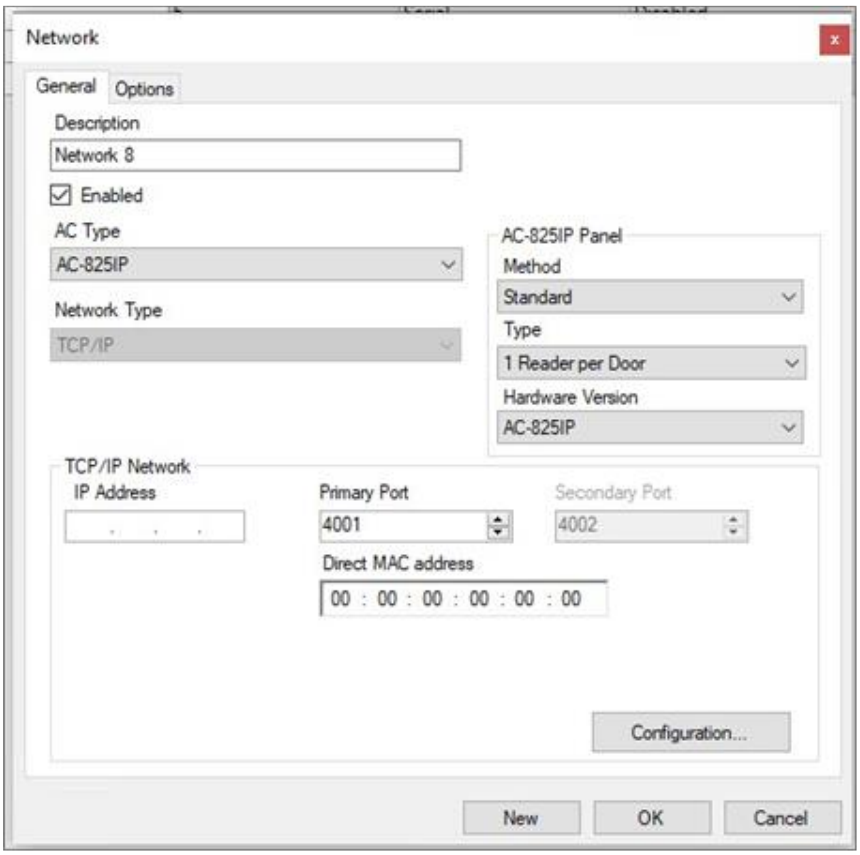
   Les panneaux sélectionnés apparaissent alors dans l'arborescence sous le réseau actuel.

Pour configurer le panneau, voir Configuration d'un panneau pour la procédure de configuration du panneau.

8.4 Ajouter un réseau pour un panneau AC-825IP

Pour ajouter un réseau à un panneau AC-825IP:

1. Sélectionnez **AC networks** dans l'arborescence.
2. Dans la barre d'outils, cliquez sur l'icône 
3. Dans **Description**, introduisez le nom du réseau..
4. Sélectionnez **Enabled**.
5. Dans **AC Type**, sélectionnez **AC-825IP**.



6. Dans la section Panneau **AC-825**
   a. Pour la **méthode OSDP**, sélectionnez Standard ou OSDP only.
   b. Sous **Type**, sélectionnez si le panneau comporte 1 ou 2 lecteurs par porte.
   c. Sous **Hardware Version**, sélectionnez s'il s'agit d'un panneau AC-825IP ou de l'une de ses extensions (R/S/D/P-805).

Une fois sélectionnés, ces paramètres ne peuvent plus être modifiés

7. Entrez l'adresse IP, le port primaire et l'adresse MAC.
8. Si vous ne connaissez pas les paramètres de connexion, cliquez sur **Configurer** pour localiser automatiquement le matériel sur le réseau local.

Pour plus d'informations sur la configuration d'une connexion TCP/IP, voir Connexion TCP/IP. Consultez votre administrateur système pour plus d'informations ou contactez le support technique Rosslare. Décochez la case Activé si vous voulez arrêter la communication avec les panneaux sur le réseau.

Les panneaux de contrôle d'accès se connectent à un réseau TCP/IP via le module intégré dans l'AC-825IP. **Consultez le Guide d'installation matérielle et d'utilisation de l'AC-825IP pour plus de détails.**

9. Cliquer sur **OK**.

Il ne peut y avoir qu'un seul panneau AC-825IP dans un réseau. Cependant, vous pouvez ajouter une carte d'extension au panneau AC-825IP (voir AC-825IP pour la procédure d'ajout d'une carte d'extension x-805) ou jusqu'à 12 extensions via RS-485..

8.5. Configurer un panneau

Chaque réseau est un regroupement de panneaux de contrôle d'accès. Dans sa forme standard, chaque panneau de contrôle d'accès peut être configuré comme un ou deux lecteurs par porte. Chacun des panneaux AC-215x et AC-225x possède deux lecteurs et peut être configuré comme un panneau à une ou deux portes. Chaque panneau AC-425x possède quatre lecteurs et peut être configuré comme un panneau à deux ou quatre portes.

En cas d'utilisation d'une carte d'extension MD-D02 (supporté par le AC-225x) ou MD-D04 (supporté par le AC-425x) en option, chaque panneau dispose de quatre ou huit lecteurs et peut être configuré comme tel.

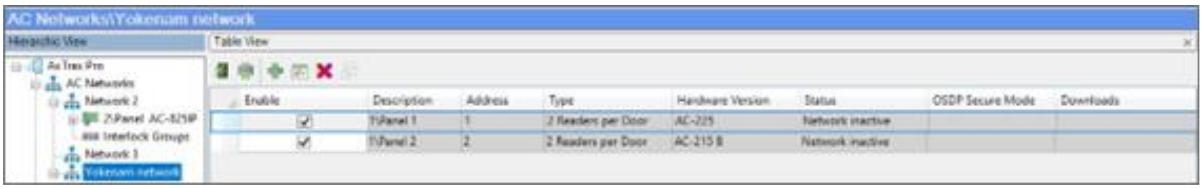
Utilisez deux lecteurs par porte lorsqu'une porte sert d'entrée et de sortie à une partie du site. Lorsque seul un lecteur d'accès est nécessaire, utilisez un lecteur par porte.

Par exemple:

- Utilisez une configuration avec deux lecteurs par porte configurés sur IN et OUT pour générer des rapports de présence.
- Utilisez une configuration avec un lecteur par porte pour contrôler deux portes avec seulement un lecteur IN (la propriété est quittée uniquement avec un interrupteur REX (Request-to-Exit) ou une poignée de porte mécanique).

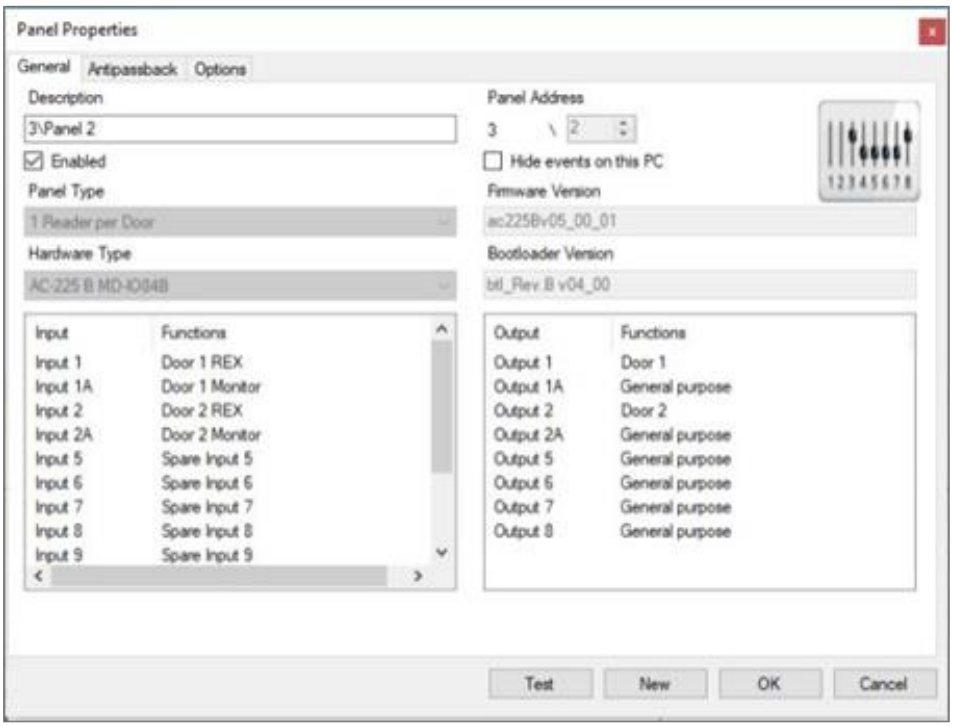
Lorsqu'il y a communication avec le panneau, les LEDs Tx et Rx clignotent.

1. Dans l'arborescence, développez l'élément AC networks et sélectionnez un réseau.
2. Sélectionnez la ligne correspondant à un panneau



3. Dans la barre d'outils, cliquez sur l'icône 

5. Dans la fenêtre **Propriétés du panneau**, sélectionnez l'onglet Général..



6. Configurez le panneau en fonction des champs décrits ci-dessous.

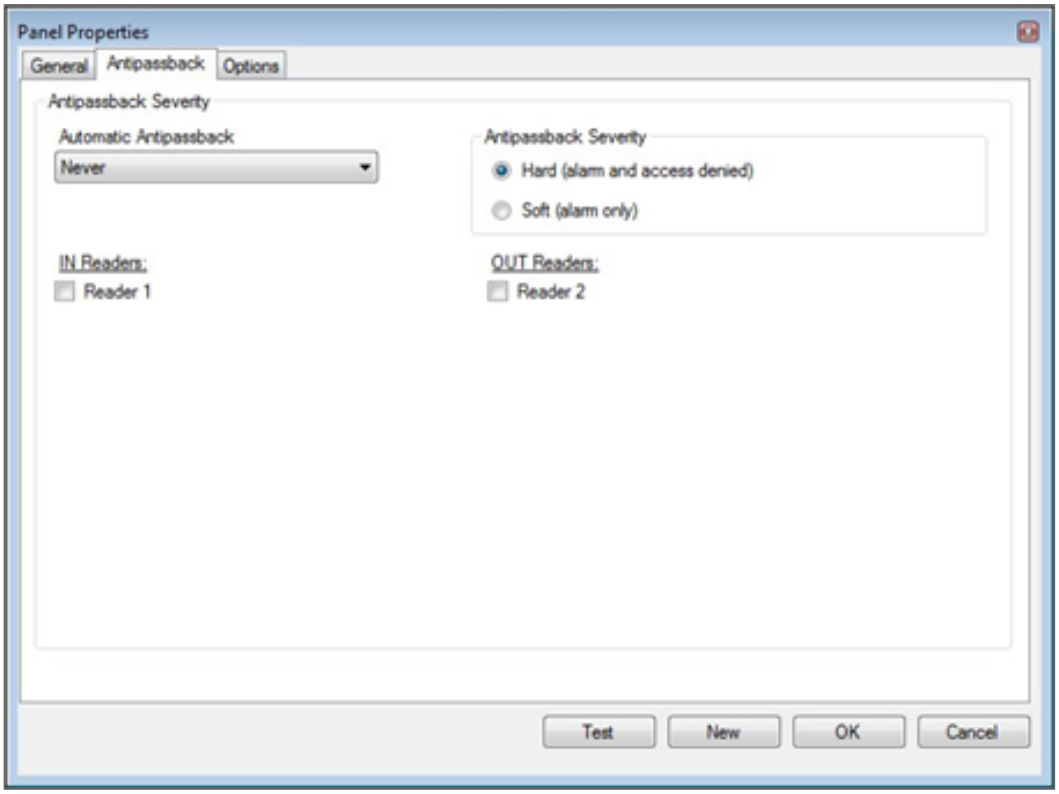
Champs	Description
Description	Entrez la description du panneau ici
Adresse du panneau	Entrez un numéro d'adresse pour le panneau. L'adresse réseau apparaît à gauche de l'adresse du panneau. Les adresses valides sont comprises entre 1 et 32.
Activé	Cochez pour activer ce panneau. Décochez si le panneau ne doit pas être connecté.
Masquer les événements sur ce PC	Cochez pour masquer les événements provenant de ce PC
Type de Panneau	Sélectionnez 1 ou 2 lecteurs par porte.
Type de matériel	Sélectionnez le type de matériel du panneau approprié
Version du micrologiciel	Après avoir sélectionné la version du matériel, le champ affiche la version actuelle du micrologiciel.
Version Bootloader	Après avoir sélectionné la version du matériel, le champ affiche la version actuelle du Bootloader.
Entrées	Affiche les connexions d'entrée du panneau
Sorties	Affiche les connexions de sortie du panneau
Test	Cliquez pour vérifier si le panneau est correctement connecté au serveur. La fenêtre Test panel affiche les détails du matériel, notamment le type de matériel, les versions du micrologiciel et du Bootloader, et indique si un lecteur ou une carte d'extension E/S est installé sur le panneau.

Assurez-vous que la position du commutateur DIP 3 sur le panneau correspond à la position indiquée dans les **propriétés du panneau**, en haut à droite de la fenêtre..

7. Cliquer sur **Test**

Si une carte d'extension est connectée au panneau de contrôle d'accès, elle apparaît sous "Carte" et un bouton Ajouter une carte est visible (voir Ajout d'une carte d'extension).

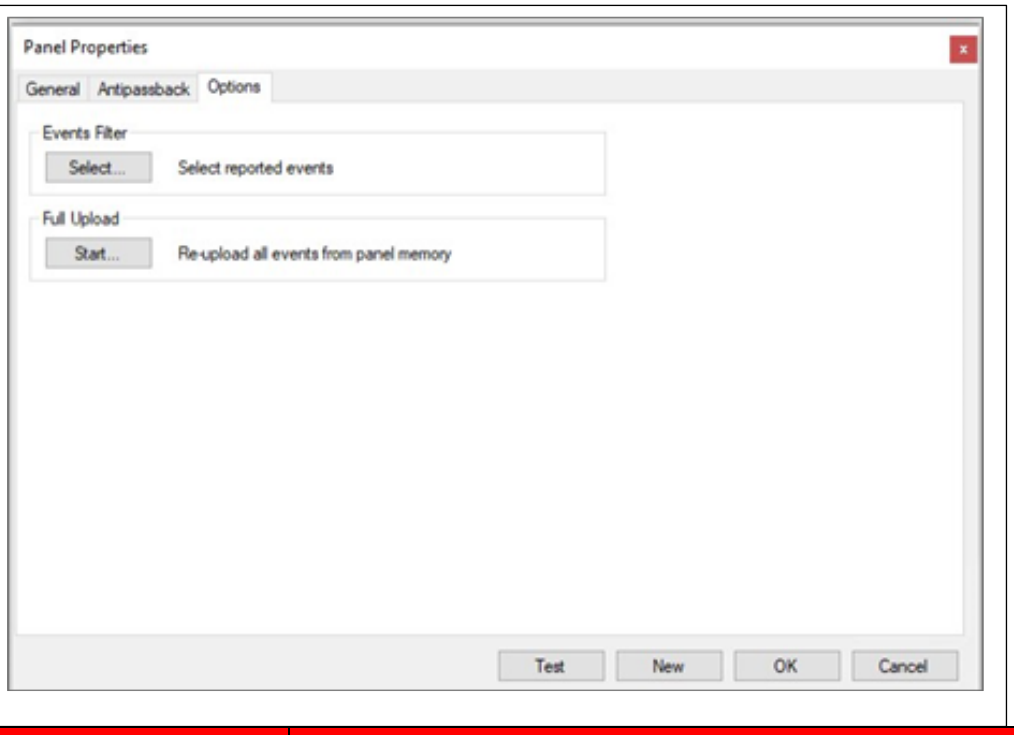
7. Cliquer sur **Close**.
8. Dans la fenêtre **Propriétés du panneau**, sélectionnez l'onglet **Antipassback.**



9. Définissez le comportement de l'anti-passback en fonction de la description des champs ci-dessous

Champs	Description
Antipassback automatique	Dans le menu déroulant AntiPassBack automatique, sélectionnez le fuseau horaire pour la porte.
Restriction de l'anti-passback	• **Hard** – Un événement est généré et la porte ne s'ouvre pas. • **Soft** – Un événement est généré et la porte s'ouvre.
Liste des lecteurs In/Out	Dans la liste des lecteurs IN/OUT, cochez les cases pour appliquer les restrictions AntiPassBack aux lecteurs si nécessaire. L'AntiPassBack du lecteur est activé lorsque la case est cochée.

10. Dans la fenêtre des **propriétés du panneau**, sélectionnez l'onglet **Options**.
11. Définissez le comportement des événements d'enregistrement en fonction des descriptions des champs ci-dessous.



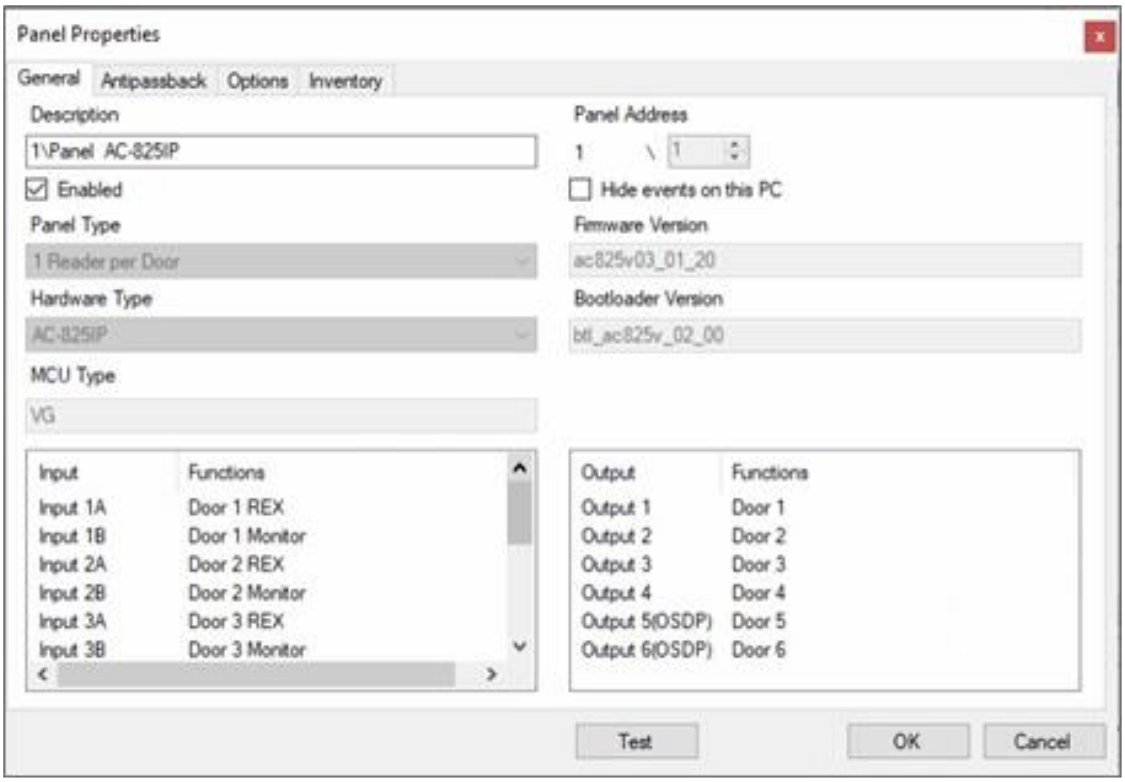
Champs	Beschrijving
Filtre des événements	Cliquez sur **Sélectionner** pour ouvrir le filtre d'événements et sélectionner les événements à enregistrer dans ce panneau. Définissez le mode de fonctionnement du filtre. Dans la configuration par défaut, certains événements sont filtrés et ont pas visibles dans Événements.
Téléchargement complet	Cliquez sur **Démarrer** pour recharger tous les événements de la mémoire du panneau. N'utilisez cette option qu'après avoir consulté le support technique Rosslare.. Un téléchargement complet peut prendre jusqu'à 3 heures.

12. Cliquer sur **OK**.

8.6. Configuration d'un panneau AC-825IP

1. Dans l'arborescence, développez l'élément Réseaux AC et sélectionnez un réseau.
2. Sélectionnez la ligne correspondant au panneau 825IP.

3. Dans la barre d'outils, cliquez sur l'icône 
4. Dans la fenêtre **Propriétés du panneau**, sélectionnez l'onglet **Général.**



5. Configurer le panneau selon les champs décrits ci-dessous

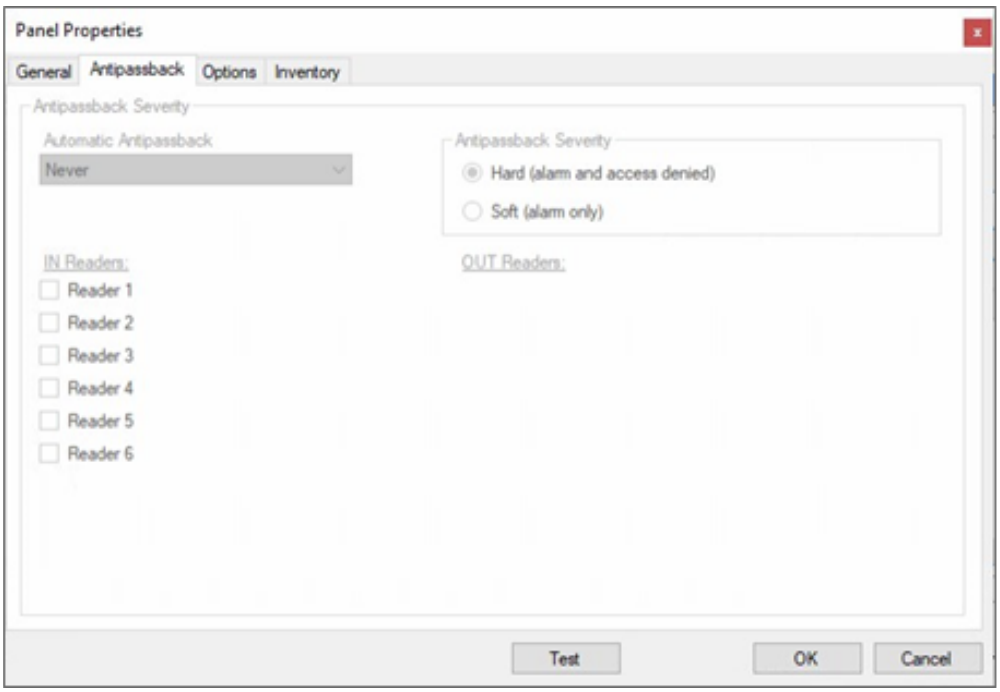
Champs	Description
Description	Entrez la description du panneau ici
Activé	Sélectionnez pour activer le panneau Décochez cette case lorsque le panneau n'est pas connecté
Masquer les événements sur ce PC	Sélectionnez cette option pour masquer les événements provenant de ce PC
Type de matériel	Sélectionnez le type de panneau approprié
Version du micrologiciel	Lorsque vous sélectionnez la version du matériel, le champ affiche la version actuelle du micrologiciel
Version du Bootloader	Lors de la sélection de la version matérielle, le champ affiche la version actuelle du Boodloader
Entrées	Affiche les connexions d'entrée du panneau
Sorties	Affiche les connexions de sortie du panneau
Test	La fenêtre Panneau de test affiche les détails du matériel, notamment le type de matériel, les versions du micrologiciel et du Boodloader, et indique si un lecteur ou une carte d'extension E/S est installé sur le panneau.

8. Cliquer sur **Test**

Si une carte d'extension est connectée au panneau de contrôle d'accès, elle apparaît sous "Carte" et un bouton Ajouter une carte est visible (voir Ajouter une carte d'extension)..

7. Cliquer sur **Close**.

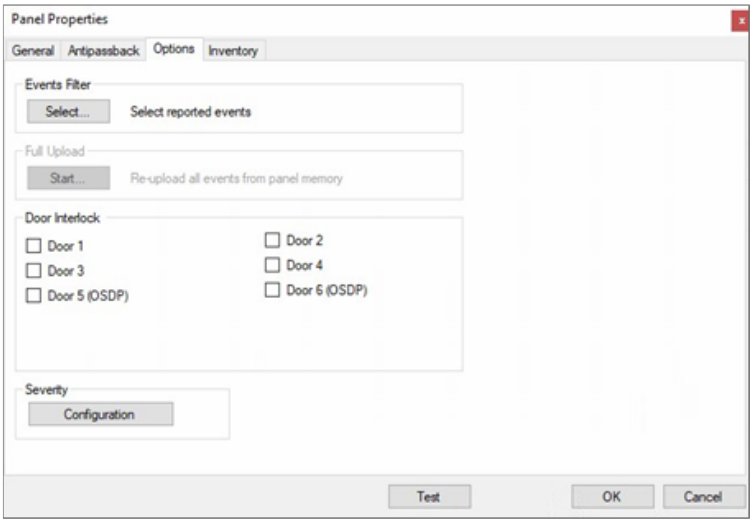
8. Dans la fenêtre **Propriétés du panneau**, sélectionnez l'onglet **Anti-passback**..



9. Définissez le comportement de l'anti-passback selon les descriptions des champs ci-dessous.

Champs	Description
Antipassback automatique	Dans le menu déroulant Antipassback automatique, sélectionnez le fuseau horaire dans lequel appliquer les règles Antipassback de la porte
Antipassback Priorité	• **Hard** - Un événement est généré et la porte ne s'ouvre pas.. • **Soft** - Un événement est généré et la porte s'ouvre.
Liste des lecteurs IN/OUT	Dans la liste des lecteurs IN/OUT, cochez les cases pour appliquer les restrictions Antipassback aux lecteurs si nécessaire. L'Antipassback du lecteur est activé lorsque la case est cochée.

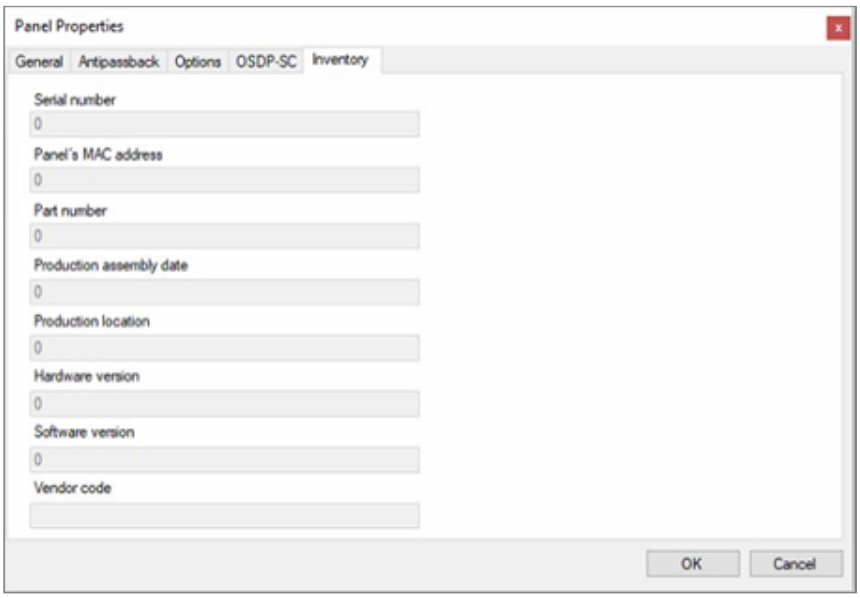
10. Dans la fenêtre **Propriétés du panneau**, sélectionnez l'onglet **Options**.



11. Définissez le comportement d'enregistrement des événements en fonction des descriptions des champs ci-dessous.

Champs	Description
Filtre d'événements	Cliquez sur Sélectionner pour ouvrir le filtre d'événements et sélectionner les événements que ce panneau doit enregistrer. Définissez le mode de fonctionnement du filtre: Dans la configuration par défaut, certains événements sont filtrés et ne sont pas visibles dans la vue Événements
Interverrouillage de la porte (Interlock)	Cette option est visible uniquement lorsque le panneau est configuré avec au moins deux portes. Cochez les cases pour appliquer la règle de verrouillage de porte aux portes concernées. Un maximum de 10 lecteurs peuvent être définis avec une règle de verrouillage de porte lorsqu'une extension D-805 est connectée à un emplacement d'extension de panneau AC-825IP. Lorsque vous utilisez une règle, assurez-vous qu'elle n'entre pas en conflit avec un groupe de verrouillage existant (voir Groupes de verrouillage). Lorsque vous utilisez une règle, assurez-vous qu'elle n'entre pas en conflit avec un groupe de verrouillage existant (voir Groupes de verrouillage). Si le lecteur a été configuré en mode carte+carte, cette fonction ne fonctionne pas dans un panneau AC-225 ou AC-425.
Urgentie	Cliquez sur Configuration pour définir le type d'urgence du journal de configuration.

2. Dans la fenêtre **Propriétés du panneau**, sélectionnez l'onglet **"Inventory".**



Champs	Description
Numéro unique du panneau	Numéro de série
Adresse MAC du panneau	Adresse MAC
Type de carte - L'application peut identifier le type de carte	Numéro de pièce
Date de montage de la production	Date d'assemblage du produit
Lieu de production	Lieu de fabrication
Changement de matériel	Changement de matériel
Version du logiciel	Version du logiciel
Code fournisseur	Pour l'utilisation de l'OSDP

13. Cliquer sur **OK**.

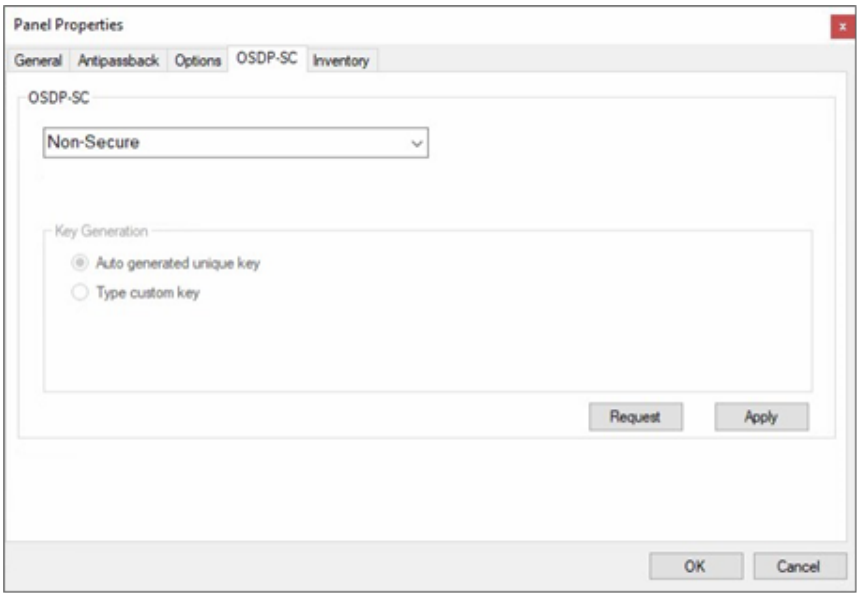
8.6.1. Onglet OSDP-SC

Cette procédure concerne les périphériques avec le protocole OSDP (Open Supervised Device Protocol). Les panneaux de commande AC-825IP prennent en charge la communication OSDP avec les unités d'extension x-805 (R/S/D/P) et 3 lecteurs OSDP.

Un panneau de commande AC-825IP peut utiliser deux appareils externes connectés au bus OSDP. Les adresses des lecteurs doivent être configurées sur 13 et 14.

La clé de l'installateur (par défaut) est utilisée pour lancer la procédure de configuration de la sécurité OSDP-Secure Channel.

1. Dans la fenêtre des **propriétés du panneau**, sélectionnez l'onglet **OSDP-SC**..
2. Sélectionnez un mode de sécurité dans la liste

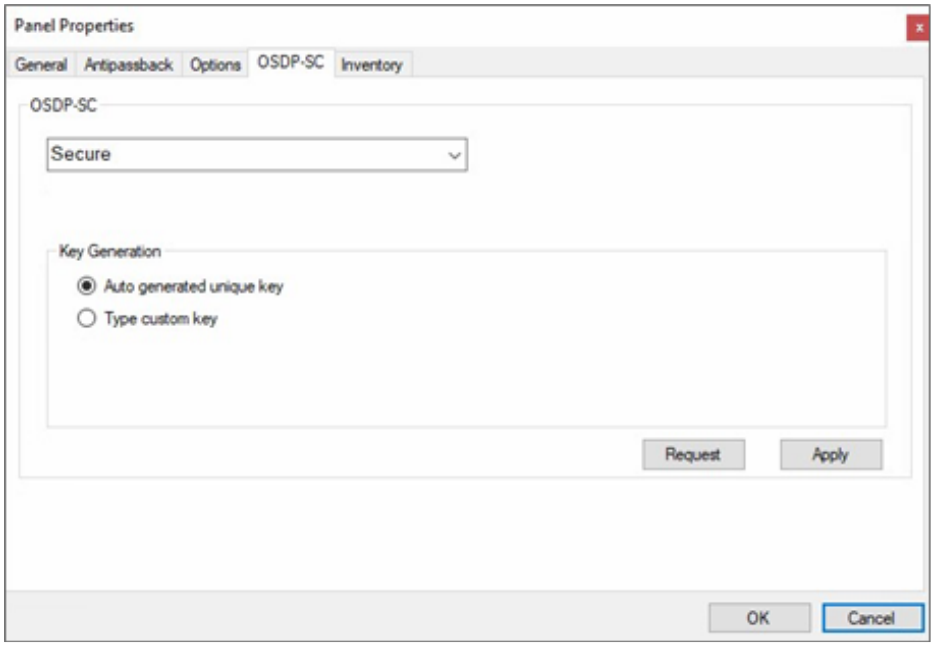


Les modes de sécurité disponibles sont les suivants:

- Non-Secure: utilisé lorsqu'aucune authentification n'est requise
- Secure: utilisé pour OSDP-Secure Channel.
- Clé par défaut - Mode d'installation : utilisé pour démarrer la communication sur le canal sécurisé

Méthode 1 : Clé unique générée automatiquement:

1. Sélectionnez **Clé unique générée automatiquement** comme **méthode de génération de clé.**



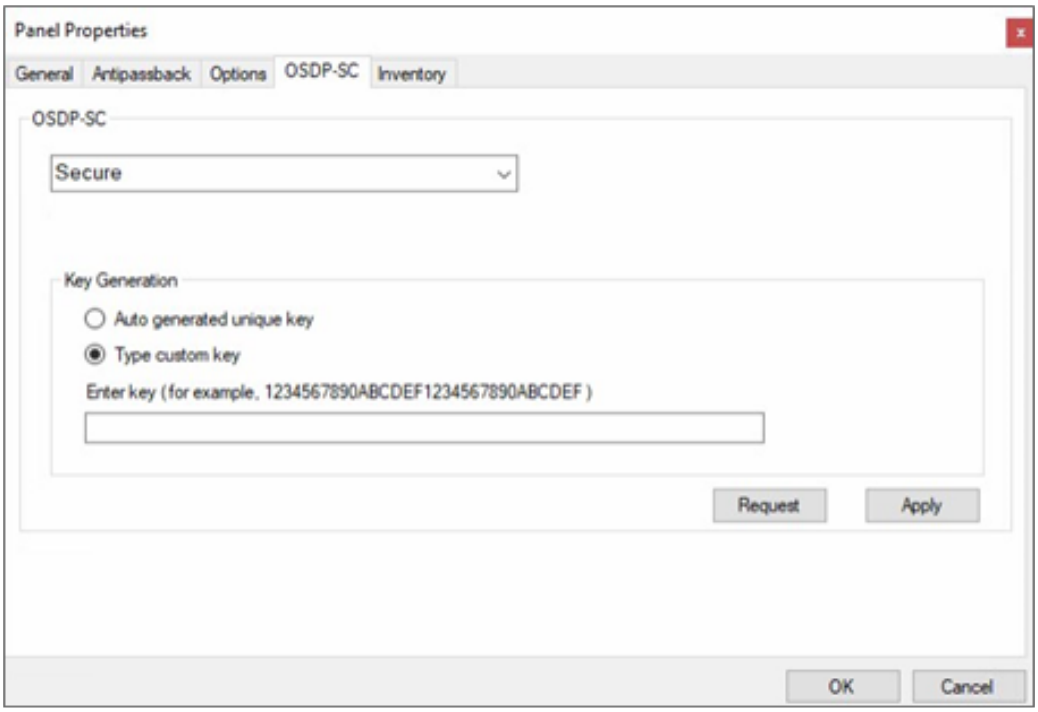
Chaque fois que cette procédure est exécutée, une clé unique et aléatoire est générée.

Il est recommandé de copier et coller la clé dans un endroit sécurisé.

2. Cliquer sur **Apply**.

Méthode 2 : Clé personnelle fournie par l'utilisateur

1. Sélectionnez **Type de clé personnalisée** pour la **méthode de génération de clé**, tapez la clé dans la zone **de saisie de la clé**.



Assurez-vous de saisir une clé de 128 bits sous forme de données hexadécimales.

2. Cliquer sur "**Apply**".

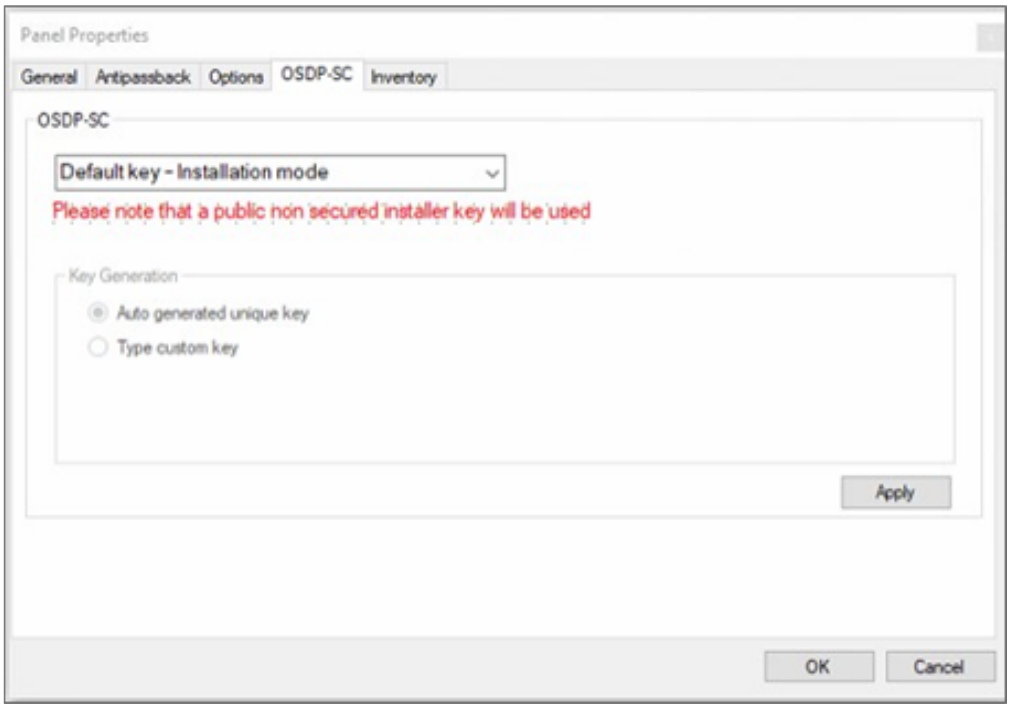
Mode installation pour démarrer la communication via le canal sécurisé

Lorsqu'il est nécessaire de reconfigurer un lecteur, utilisez la clé **sécurisée - par défaut (mode installation)** pour réinitialiser le lecteur.

Lorsque l'option **Clé par défaut - mode installation** est sélectionnée, tous les matériels concernés doivent être configurés en mode installation.

1. Sélectionner la **clé par défaut - Mode d'installation** d'une **méthode de sécurité.**

> Après avoir sélectionné une clé par défaut, la communication n'est pas sécurisée. Cela est dû au fait que la clé par défaut est une clé d'installation publique et non sécurisée.



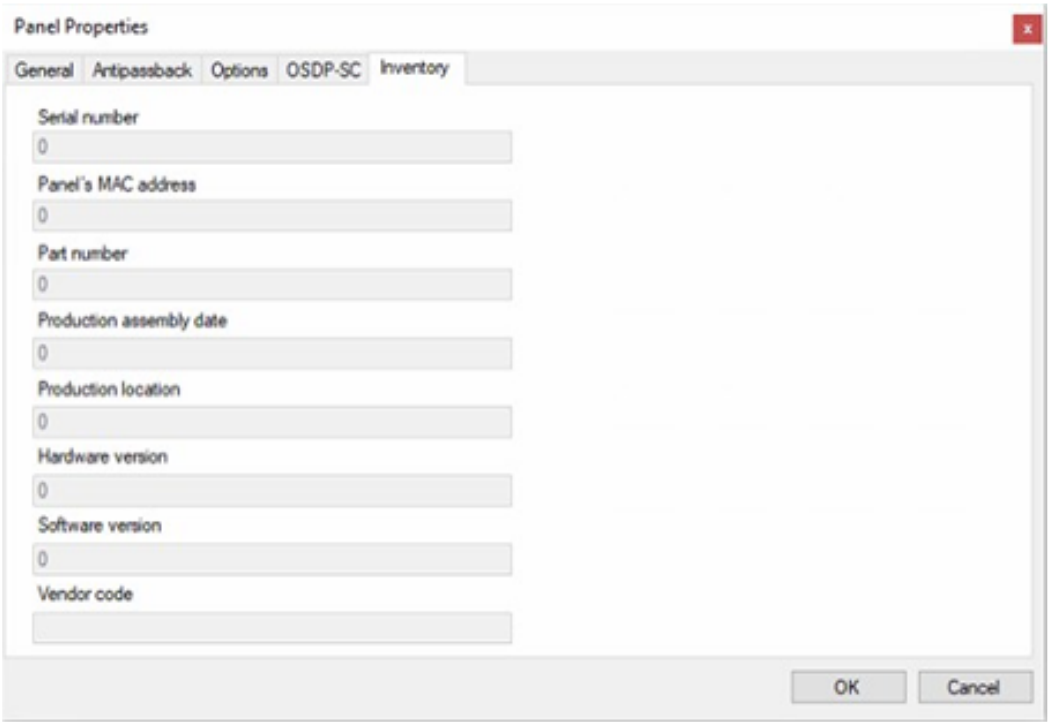
2. Cliquer sur "**Request"**.
3. Cliquer sur "**Apply"**.
4. Configurez l'OSDP en utilisant la méthode 1 : Clé unique générée automatiquement.

   ou

5. Configurez le PPO avec la méthode 2 : User Provided Custom Key (Clé personnalisée fournie par l'utilisateur).

8.6.2. Onglet Inventaire

1. Dans la fenêtre du **panneau,** sélectionnez l'onglet **"Inventaire".**



Champs	Description
Numéro unique du panneau	Numéro de série
Adresse MAC du panneau	Adresse MAC
Type de carte - L'application peut identifier le type de carte	Numéro de pièce
Date de montage de la production	Date d'assemblage du produit
Lieu de production	Lieu de fabrication
Changement de matériel	Changement de matériel
Version du logiciel	Version du logiciel
Code fournisseur	Pour l'utilisation de l'OSDP

2. Cliquer sur **OK**.

8.6.3. Groupes Interlock

Des groupes de verrouillage (Interlock), peuvent être définis pour les panneaux AC-825IP. Un groupe de portes peut être sélectionné pour être activé en mode interlock, ce qui signifie qu'une seule porte peut être ouverte à la fois.

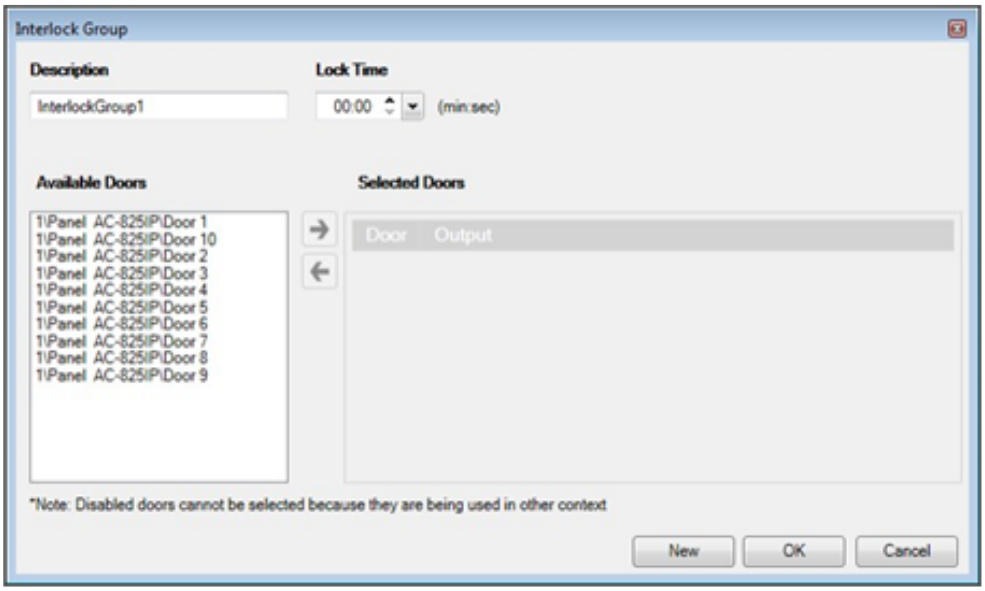
Une porte peut être sélectionnée dans jusqu'à 5 groupes de verrouillage différents.

Une minuterie peut être définie au cas où le mode de verrouillage serait activé après la fermeture de la porte. Toutes les portes du groupe sont désactivées pendant cette période.

Lorsque vous définissez un groupe d'interlock, assurez-vous qu'il n'entre pas en conflit avec une règle d'interlock existante, voir Porte Interlock.

Pour ajouter un groupe d'interlock:

1. Dans l'arborescence, développez un réseau AC-825IP.
2. Sélectionnez **Groupes d'interlock..**
3. Dans la barre d'outils, cliquez sur l'icône 



4. Sélectionnez et déplacez les portes souhaitées de Portes disponibles à Portes sélectionnées à l'aide des flèches.
5. Cliquez sur **OK**.

La fenêtre se ferme et le nouveau groupe d'interlocks apparaît dans la zone d'affichage.

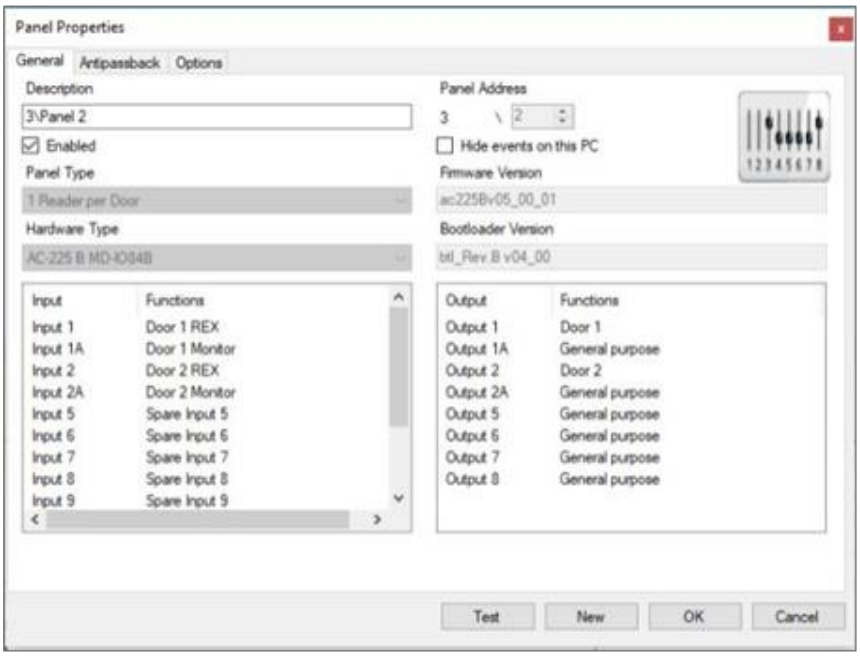
8.7. Ajouter une carte d'extension

8.7.1. AC-225x et AC-425x

Pour les panneaux AC-225x, vous pouvez ajouter une carte d'extension MD-D02 ou MD-IO84 par panneau de contrôle d'accès.
Pour les panneaux AC-425x, vous pouvez ajouter une carte d'extension MD-D04 ou MD-IO84 par panneau de contrôle d'accès.

Pour ajouter une carte d'extension:

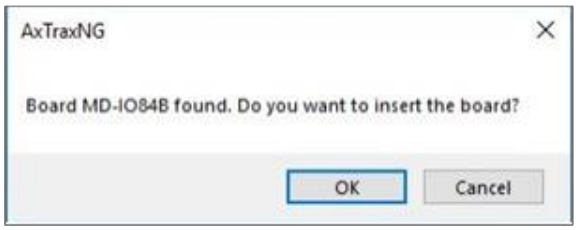
1. Mettez le panneau hors tension.
2. Insérer la carte d'extension dans le panneau et remettez l'alimentation de la carte sous tension.
3. Dans **l'arborescence**, déployez l'élément **AC Networks** et sélectionnez un réseau.
4. Dans la barre d'outils, cliquez sur l'icône 



5. Cliquer sur “**Test**”.

6. Cliquer sur “**Add Board”**.

Après quelques instants, la confirmation suivante apparaît:



7. Cliquer sur **OK**.

La fenêtre se ferme et le nouveau panneau apparaît dans la zone d'affichage.

Pour retirer une carte d'extension d'un panneau, vous devez retirer le panneau de la base de données.

8.7.2. AC-825IP

Vous pouvez ajouter une carte d'extension x-805 au panneau AC-825IP.

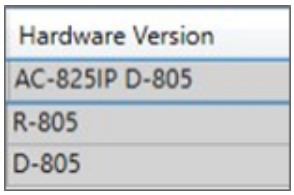
Une seule carte d'extension peut être insérée par panneau de contrôle d'accès.

Pour ajouter une carte d'extension:

1. Mettez le panneau hors tension.
2. Connecter la carte d'extension au panneau et remettre l'alimentation de la carte sous tension.

Pour ajouter une carte d'extension AC-825 avec D-805 dans une topologie en chaîne, il est nécessaire de spécifier la configuration **AC-825IP/D-805**. Cette configuration n'est pas ajoutée automatiquement..

Une fois que le panneau AC-825IP est connecté, vous verrez dans la colonne Hardware Version de l'arborescence que la carte d'extension est installée.



Pour retirer une carte d'extension d'un panneau, supprimez le panneau de la base de données.

8.8. Retirer un panneau

Pour retirer les panneaux installés en périphérie:

1. Dans l'arborescence, déployez l'élément **AC Networks**
2. Déployez un réseau et déployez un panneau.
3. Sélectionnez la ligne du panneau à supprimer.
4. Cliquer sur
5. Cliquer sur **Yes**.

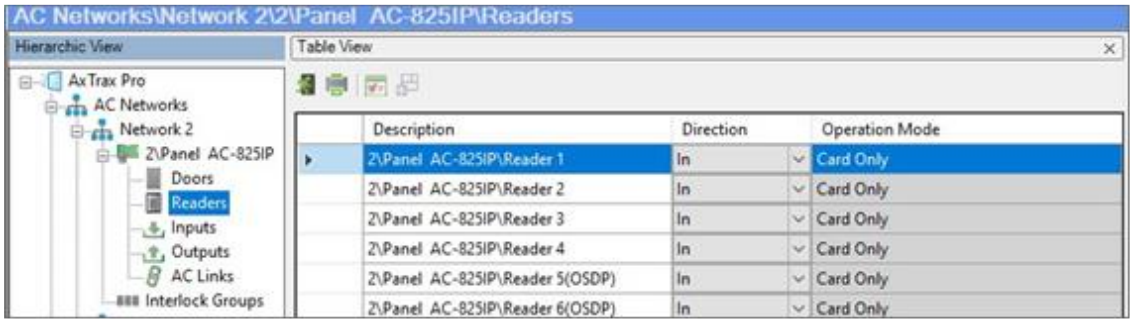
Le journal des événements affiche **"Succeed"** pour le panneau qui a été supprimé

8.9. Configuration d'un lecteur

Un panneau peut être connecté à deux, quatre ou huit lecteurs lorsque les cartes d'extension MD-D02 ou MD-04 sont connectées.

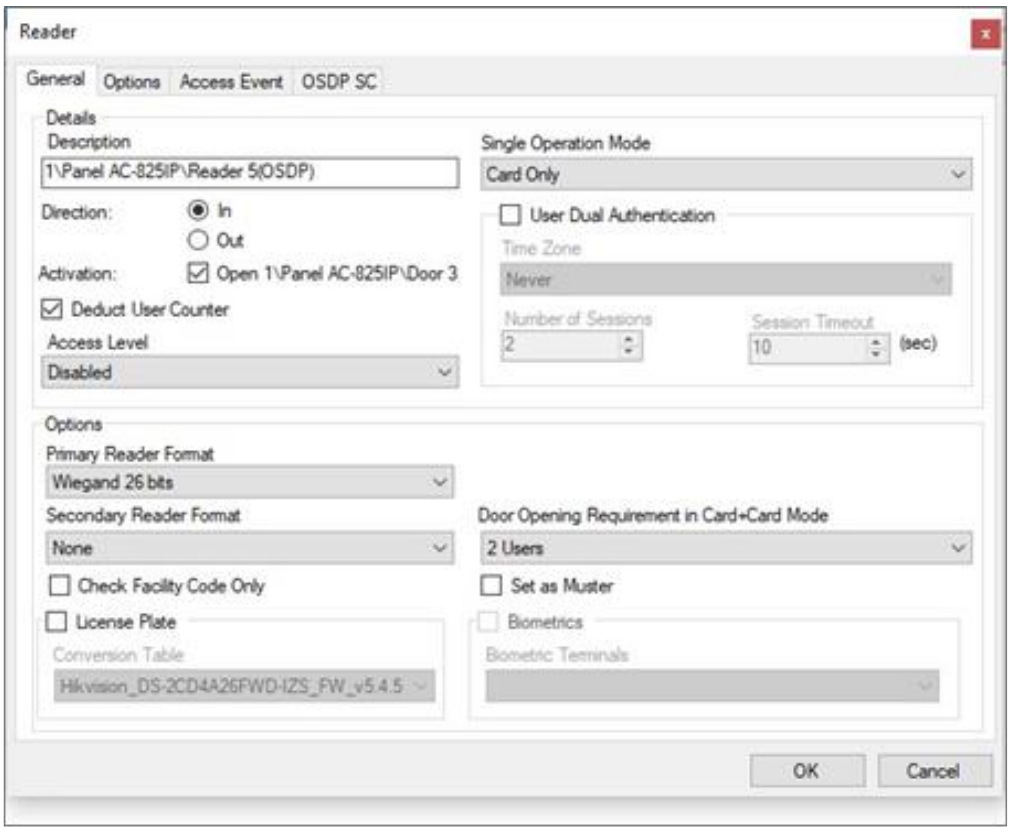
8.9.1. Onglet Général

1. Dans l'arborescence, déployer l'élément AC Networks et sélectionner un réseau.
2. Sélectionnez un panneau et un lecteur.
3. Sélectionnez une ligne d'un lecteur.



4. Dans la barre d'outils, cliquez sur l'icône

5. Dans la fenêtre **"lecteur",** sélectionnez l'onglet **Général.**



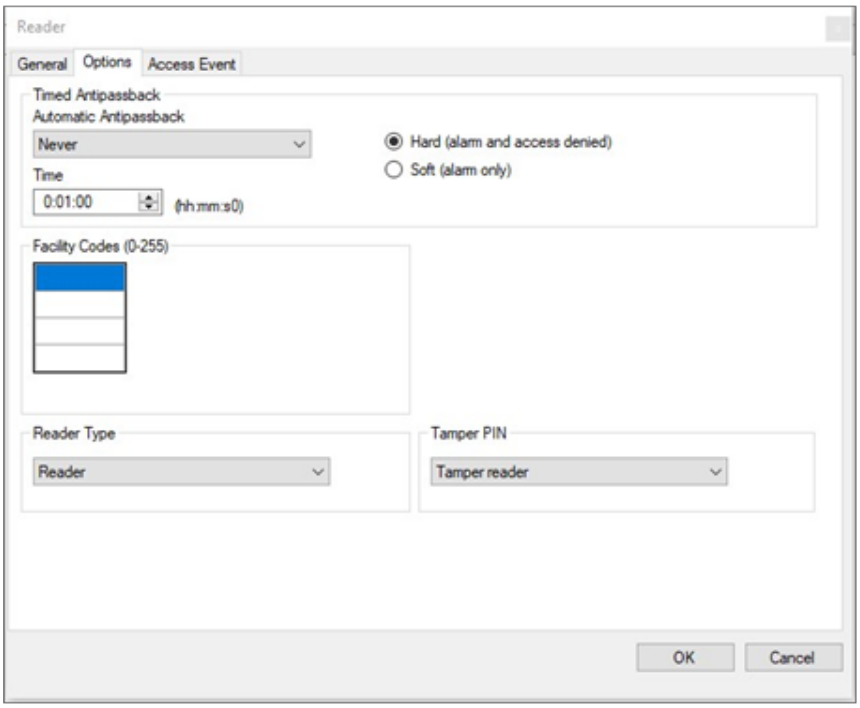
6. Définissez les propriétés du lecteur conformément aux descriptions des champs dans le tableau suivant

Champs	Description
Détails > Direction	Choisir si le lecteur permet d'entrer ou de sortir de la zone.
Détails > Activation	Sélectionnez si le lecteur est autorisé à déverrouiller la porte. Si cette option est sélectionnée, la sortie de la porte est active tant qu'un utilisateur valide est présent. Si la case n'est pas cochée, les événements enregistrés sont reçus en ligne et apparaissent dans la barre d'outils Événements.
Détails > Soustraction du compteur de l'utilisateur	Sélectionnez cette option pour enregistrer cette entrée dans le compteur de droits d'accès de l'utilisateur.
Détails > Niveau d'accès	Sélectionner le niveau d'accès
Détails > Mode de fonctionnement unique	Sélectionnez le mode de fonctionnement du lecteur: • **Inactif**: le lecteur n'est pas utilisé • **Carte uniquement:** Le lecteur fonctionne uniquement avec des cartes RFID**.** • **PIN uniquement:** le lecteur fonctionne uniquement avec un code PIN**.** • **Carte ou code PIN:** le lecteur dispose à la fois d'un lecteur de carte et d'un code PIN. • **Desktop:** le lecteur n'est pas actif, mais il est utilisé pour programmer de nouvelles cartes dans le logiciel.. • **Pas d'accès:** le lecteur ne donne pas accès à tous les utilisateurs. • **Carte + Carte**: Le lecteur donne accès lorsque deux utilisateurs différents présentent leur carte devant le lecteur.
Double authentification des utilisateurs	Sélectionnez cette option pour activer le mode de double authentification, qui impose 2 justificatifs d'identité par utilisateur et par accès

	Un maximum de 10 lecteurs dans un réseau peut être défini avec la double authentification.
Double authentification de l'utilisateur > Fuseau horaire	Sélectionnez le fuseau horaire dans lequel la double authentification est active • **Toujours (par défaut)** • **Jamais** • **N'importe quel(s) fuseau(x) horaire(s) précédemment défini(s) dans le système**
Authentification double utilisateur > Nombre de sessions	Sélectionnez cette option pour définir le nombre de sessions disponibles Une session est la période pendant laquelle deux informations d'identification sont présentées par utilisateur pour un accès unique. • **1 (par défaut)** • **2 (uniquement pour les panneaux AC-825IP)**
Authentification double utilisateur > Délai d'attente de la session	Durée en secondes de chaque session La plage est comprise entre 5 et 255 (la valeur par défaut est 10).
Options > Format du lecteur primaire	Sélectionner le type de transmission de données pour le matériel primaire du lecteur
Options > Format du lecteur secondaire	Sélectionnez le type de transmission de données pour le lecteur secondaire. Ce champ est utilisé lorsque deux types de cartes différents sont utilisés
Options > Type de clavier	Sélectionnez le type de transmission de données pour le type de clavier.
Options > Ouverture de porte requise en mode carte + carte	Sélectionnez 2 ou 3 utilisateurs nécessaires pour ouvrir la porte en mode Carte + Carte. Dans l'AC-215A, cette fonction est désactivée.
Options > Vérification du code de l'établissement uniquement	Sélectionnez cette option pour accorder l'accès à tout utilisateur assigné à un établissement dans la liste d'établissements sélectionnée. La liste des établissements est définie dans l'onglet Options. Cette option n'est disponible que pour certains formats.
Plaque d'immatriculation	Cochez cette case pour autoriser l'utilisation d'une table de conversion personnalisée.
Plaque d'immatriculation > Table de conversion	Sélectionnez la table de conversion appropriée.
Options > Définir comme Muster	Cochez cette case pour permettre le suivi du personnel accrédité.
Biométrie	Cochez la case pour attribuer un lecteur à un terminal (voir À partir d'un réseau distant).

8.9.2. Onglet Options

1. Dans la fenêtre "**Lecteur",** sélectionnez l'onglet **Options**.

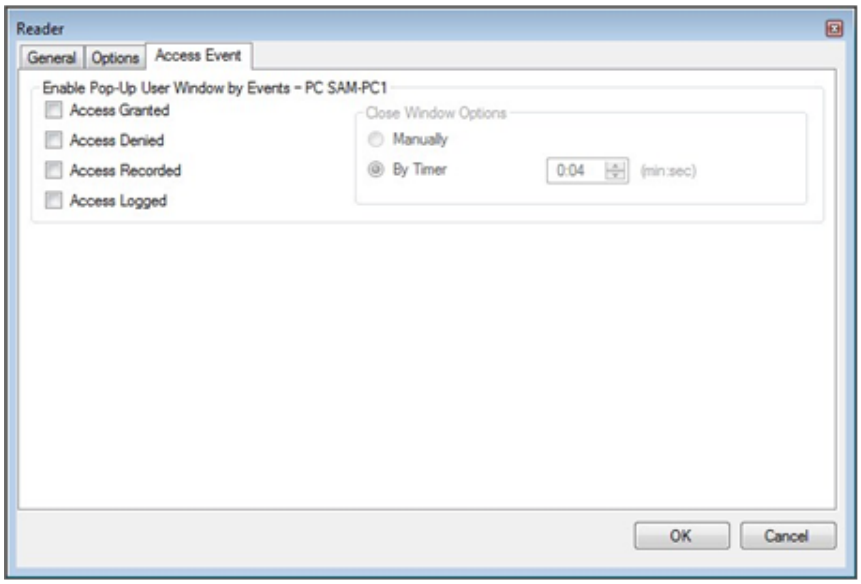


2. Définissez les propriétés en fonction de la description des champs dans le tableau suivant:

Champs	Description
Automatic Antipassback	Choisissez d'appliquer ou non des règles anti-passback. Pour ajouter un fuseau horaire, voir Ajouter des fuseaux horaires.
Hard	Lorsque l'option Antipassback "dur" est sélectionnée, un événement est généré et la porte ne s'ouvre pas.
Soft	Lorsque l'option Antipassback "doux" est sélectionnée, la porte s'ouvre, mais un événement est également généré.
Timed Antipassback	Définissez le nombre de minutes pendant lesquelles un utilisateur peut entrer à nouveau après avoir badgé sur ce lecteur..
Facility codes	Cliquez sur et tapez le code facilité (entre 0 et 255). Il est possible de saisir jusqu'à quatre codes d'installation différents.
Reader Type	Sélectionnez le type de lecteur.
Tamper PIN	Sélectionnez le code PIN pour l'autoprotection.

8.9.3. Événement d'accès

Dans la fenêtre **"lecteur",** sélectionnez l'onglet **Événement d'accès**.



1. Définissez les propriétés en fonction de la description des champs dans le tableau suivant:

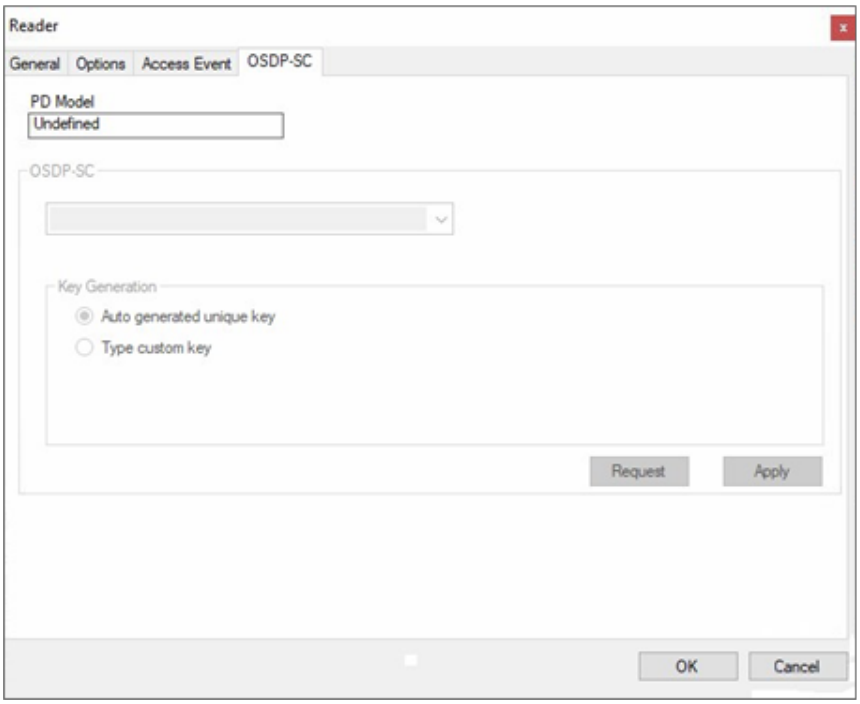
Champs	Description
Access Granted	Sélectionnez cette option pour activer une fenêtre contextuelle pour une alarme de type "Accès autorisé".
Access Denied	Sélectionnez cette option pour activer une fenêtre contextuelle pour une alerte de type "Accès refusé".
Access Recorded	Sélectionnez cette option pour activer une fenêtre contextuelle (pop-up) pour les alertes de type événement d'accès enregistré.
Access Logged	Sélectionnez cette option pour activer une fenêtre contextuelle (pop-up) pour les alertes de type Accès à un événement enregistré (Access Logged).
Close Windows Options	Lorsqu'une fenêtre contextuelle (pop-up) est activée, des options de fermeture de la fenêtre sont disponibles. Sélectionnez l'une des deux options suivantes : •**Manuelle** : l'opérateur doit fermer la fenêtre contextuelle (pop-up) manuellement. •**Par minuterie** : la fenêtre contextuelle (pop-up) se ferme automatiquement en fonction de la minuterie prédéfinie.

8.9.4. Onglet OSDP-SC

Cette procédure concerne les lecteurs avec Open Supervised Device Protocol (OSDP).

Les adresses des lecteurs doivent être définies sur 13 et 14..

1. Dans la fenêtre "**Lecteur",** sélectionnez l'onglet **OSDP-SC.**
2. Sélectionnez un **"PD Model**" dans la zone de liste..



3. Cliquer sur "**Apply"**.

Installation pour reconfigurer un lecteur

S'il est nécessaire de reconfigurer un lecteur, suivre la procédure décrite dans la section Configuration d'un panneau AC-825IP.

8.10. Ajouter un terminal biométrique

Vous pouvez ajouter un terminal biométrique à un réseau en utilisant l'élément **Biométrie.**

Un terminal biométrique peut être utilisé pour lire et transmettre des informations d'identification ou pour enregistrer de nouvelles informations d'identification (empreintes digitales et Cartes/Tags).

Les terminaux prennent en charge les protocoles TCP/IP et Wiegand.

Ajouter un terminal biométrique peut se faire soit sur un réseau local, soit à partir d'un réseau distant.

8.10.1 Dans un réseau local

Pour ajouter un terminal biométrique dans un réseau local:

1. Dans l'arborescence, développez l'élément “**Biometrics’’** et sélectionnez **‘’Terminals’’**.

2. Dans la barre d'outils, cliquez sur l'icône 

3. Dans **Description**, entrez le nom du nouveau terminal.
4. Sélectionnez **Enabled** (Activé) pour activer le terminal..
5. Dans **Model Number**, sélectionnez le modèle de lecteur.
6. Dans la zone **Réseau TCP/IP**, entrez l'adresse MAC, l'adresse IP et le port.

Pour les modèles AY-B9250BT et AY-B9350, une case à cocher supplémentaire "enable snapshot camera" apparaît. Si cette case est cochée, le terminal prend un instantané de l'écran du terminal.

Pour la série Bio9000, il existe une option "Live fingerprint detection" (détection d'empreintes digitales en direct)

Si vous activez cette option, vous pouvez vous attendre à un temps de reconnaissance plus long et à un taux de reconnaissance plus faible. taux de reconnaissance plus faible

7. Cliquer sur **OK**.

La fenêtre se ferme et le nouveau terminal apparaît dans la zone d'affichage.

Si vous ne connaissez pas les paramètres de connexion, cliquez sur **Configurer** pour rechercher du matériel sur le réseau local. Consultez le guide Configuration d'un terminal biométrique pour savoir comment rechercher et configurer un terminal biométrique..

8.10.2. Depuis un réseau distant

Pour ajouter un terminal biométrique à partir d'un réseau distant, vous devez d'abord recevoir un fichier exporté du réseau distant qui contient tous les paramètres de configuration du terminal. Une fois ce fichier reçu, vous pouvez ajouter le terminal biométrique en important ce fichier.

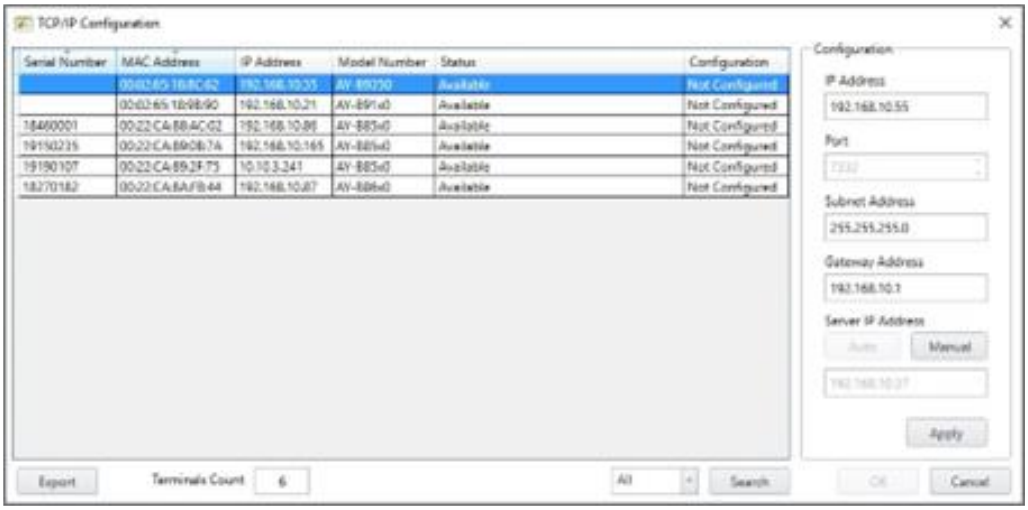
8.10.2.1. Exporter un fichier de terminal

Pour exporter un fichier de terminal:

1. Dans l'arborescence, développez l'élément **Biométrie** et sélectionnez **Terminaux**.

2. Dans la barre d'outils, cliquez sur l'icône 

3. Cliquer sur **Configuration**.
4. La fenêtre de **configuration TCP/IP** s'ouvre et recherche automatiquement tout terminal connecté au réseau..



5. Cliquez sur **Exporter.**
6. Dans la fenêtre **Enregistrer sous**, saisissez le nom du fichier et enregistrez le fichier (xxx.axbio) sur votre PC, où il sera facilement accessible.

La fonction Export ajoute "axbio" à la fin du nom du fichier exporté. La fonction Import ne s'exécute qu'avec un fichier contenant cette chaîne à la fin du nom de fichier.

8.10.2.2. Importation d'un fichier de terminal

Pour importer un fichier de terminal:

1. Dans l'arborescence, développez l'élément **Biométrie** et sélectionnez **Terminaux**.
2. Dans la barre d'outils, cliquez sur l'icône 

   La fenêtre **Importer un terminal** s'ouvre..
3. Recherchez le fichier xxx.axbio précédemment exporté et double-cliquez dessus.

La fenêtre se ferme et le terminal apparaît dans la zone d'affichage.

8.10.3. Configuration d'un terminal biométrique

Le serveur AxTraxPro communique avec un terminal biométrique de deux manières : TCP/IP (LAN ou WAN) et le protocole Wiegand.

Chaque terminal a une adresse MAC unique et apparaît séparément dans le système.

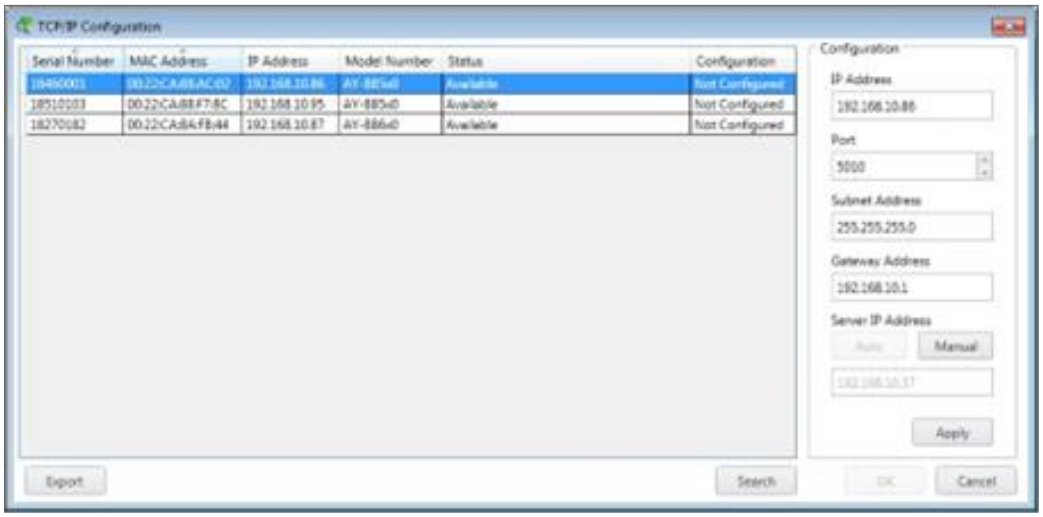
Le serveur AxTraxPro supporte plusieurs terminaux par réseau de contrôle d'accès.

Pour rechercher le terminal biométrique à configurer:

1. Dans l'arborescence, développez l'élément **Biométrie** et sélectionnez **Terminaux**.

2. Dans la barre d'outils, cliquez sur l'icône 
3. Cliquer sur **Configuration**.

La fenêtre **Configuration TCP/IP** s'ouvre et recherche automatiquement les terminaux connectés au réseau..



La fenêtre principale affiche tous les terminaux connectés au réseau local et indique s'ils ont été préalablement affectés à un terminal ou non.

Pour un terminal biométrique qui n'a pas encore été configuré:

1. Sélectionnez le terminal en question.

   Les paramètres du terminal sont affichés dans la **zone Configuration** à droite.

2. Cliquer sur **Apply**.

   Attendez que la liste se rafraîchisse et regardez que le statut du terminal est maintenant **Configuré.**

3. Sélectionnez à nouveau le terminal dans la liste
4. Cliquer sur **OK**.

La fenêtre se ferme et le nouveau terminal apparaît dans la zone d'affichage.

8.10.4. Associer un terminal biométrique à un lecteur

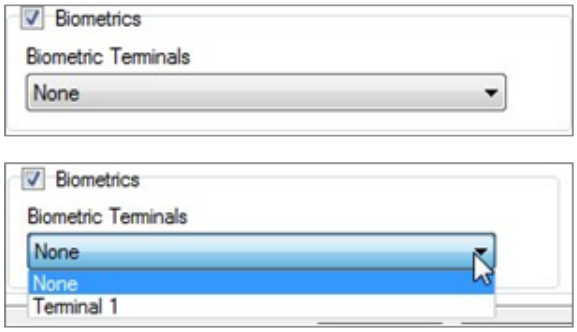
Une fois que vous avez ajouté un terminal biométrique au système, vous devez l'associer à un lecteur spécifique afin que le système puisse reconnaître le terminal.

Pour associer un terminal biométrique:

1. Dans l'arborescence, développez l'élément **AC Networks.**
2. Développez un réseau et développez un panneau.
3. Sélectionnez Lecteurs (**Readers)**.

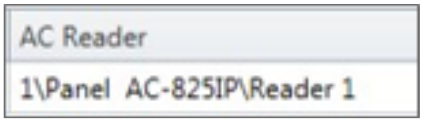
   Les lecteurs disponibles sont affichés dans la zone d'affichage.
4. Sélectionnez un lecteur dans la zone d'affichage.
5. Dans la barre d'outils, cliquez sur l'icône 

   La fenêtre **Reader Properties** s'ouvre dans l'onglet "**General"**.
6. Cochez la case Biométrique et sélectionnez le terminal concerné dans le menu déroulant.



7. Cliquez sur **OK** pour accepter les modifications

   Lorsque vous sélectionnez l'élément **Termina**l, vous pouvez maintenant voir dans la zone d'affichage à quel lecteur le terminal est assigné..

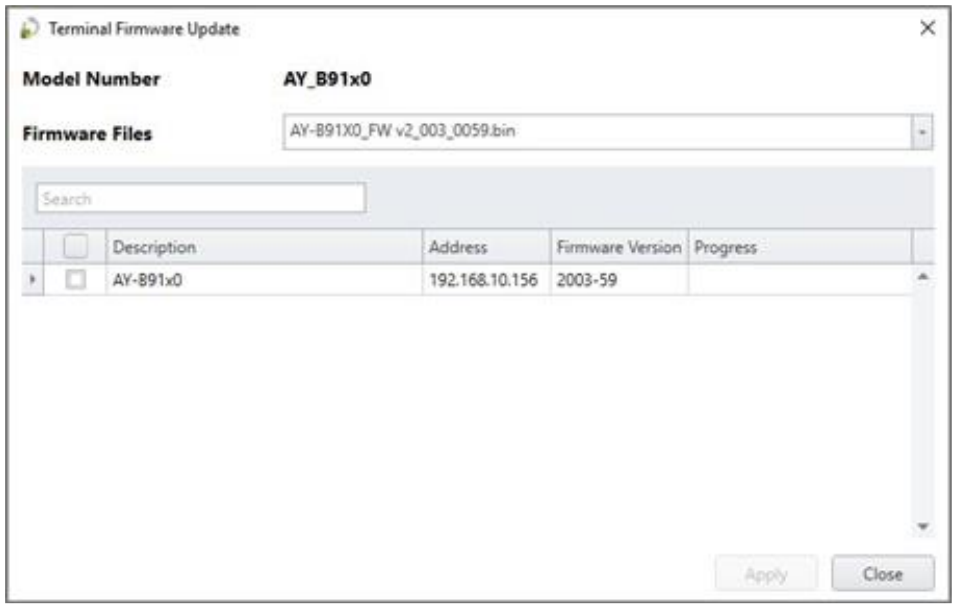


8.10.5. Mise à jour du micrologiciel à partir du terminal

Pour mettre à jour le micrologiciel:

Cette fonction n'est disponible que pour la série 9000 Biométrique.

1. Dans l'arborescence, développez **Biometrics > Terminals.**
2. Sélectionnez un terminal.
3. Dans la barre d'outils, cliquez sur l'icône 



4. Vérifier le(s) terminal(aux) dans la liste
5. Cliquer sur **Apply**.
6. Attendez la fin du processus et cliquez sur **Close** (Fermer).

8.11. Configuration des portes

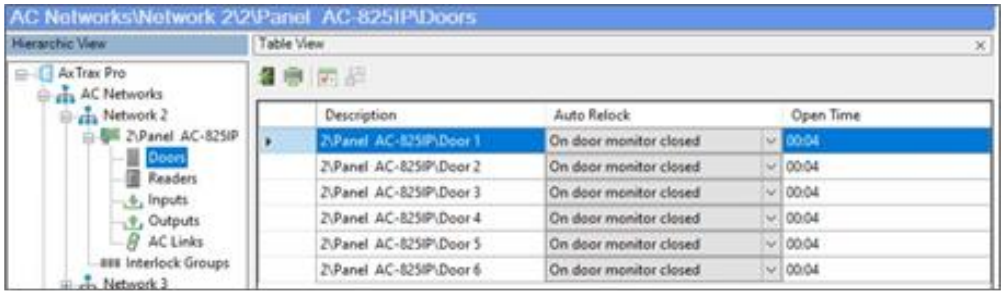
Chaque panneau contrôle de une à huit portes. Chaque porte peut être configurée individuellement.

La fenêtre **"Door**" (porte) affiche les éléments suivants :

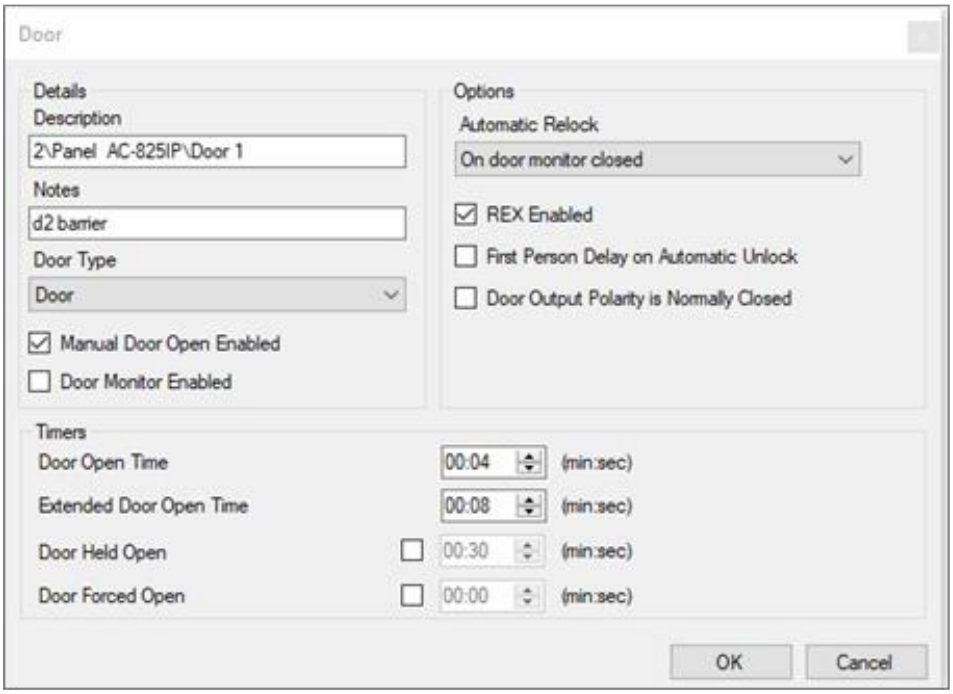
- Les paramètres de déverrouillage et de verrouillage.
- Le temps disponible avant que la porte ne se déverrouille ou n'enregistre des alarmes.

Pour modifier les propriétés de la porte:

1. Dans l'arborescence, développez l'élément **AC Networks**.
2. Développez un réseau et développez un panneau.
3. Sélectionnez “**Doors”**.
4. électionnez une porte dans la zone d'affichage.



5. Dans la barre d'outils, cliquez sur l'icône 



6. Configurez la porte en fonction des champs du tableau suivant:

Champs	Description
Description	Entrez le nom de la porte
Remarque	Écrivez éventuellement des commentaires ici
Type de porte	Sélectionnez le type de porte
Verrouillage automatique	Sélectionnez l'événement qui provoque le verrouillage automatique de la porte
REX activé (Bouton-Poussoir de sortie)	Une demande de sortie déverrouille la porte pour une durée définie par l'utilisateur. Sélectionnez cette option pour autoriser le REX pour cette porte. L'emplacement de l'entrée REX dépend de la configuration du panneau ; il est indiqué dans la fenêtre Propriétés du panneau.
Délai pour la première personne lors du déverrouillage automatique	Définit le comportement de la porte pendant une plage horaire pour le déverrouillage automatique. Sélectionnez cette option pour exiger que, pendant la plage horaire sélectionnée, la porte reste verrouillée jusqu'à ce que le premier utilisateur l'ouvre. La zone horaire de déverrouillage automatique est sélectionnée dans les liens de panneau en sélectionnant la sortie correspondant à cette porte (voir **Ajouter des liens de panneau**).
La polarité de la sortie de porte est normalement fermée	Sélectionnez cette option pour garantir l'ouverture de la porte en cas de défaillance de l'alimentation de la serrure de la porte. Après la mise sous tension, le relais de porte est activé lorsque la porte est fermée et désactivé lorsque la porte est ouverte. Dans cette configuration, la serrure de sécurité doit être connectée aux bornes N.O. (Normal Open) et COM (Common) du relais de porte.
Ouverture manuelle de la porte activée	Sélectionnez cette option pour permettre aux opérateurs de configurer la porte manuellement (voir Add panel links).
Surveillance de la porte activée	Sélectionnez cette option pour surveiller la porte.
Temps d'ouverture de la porte	Programmer la durée pendant laquelle la porte reste déverrouillée.
Temps d'ouverture de la porte prolongé	Configurez la durée pendant laquelle la porte reste déverrouillée pour les utilisateurs disposant de droits d'ouverture de porte étendus.
Porte laissée ouverte trop longtemps	Définir la durée pendant laquelle la porte peut être maintenue ouverte sans qu'un événement d'alarme ne se produise. Sélectionnez pour utiliser cette minuterie. Pour l'application serveur, la section Pop-up Snapshot s'ouvre. Si cette fonction est activée, le délai de démarrage de l'activité (voir : **Ajout d'un terminal biométrique**) doit être mis à **0** pour cette porte.
Ouverture forcée de la porte	Définir la durée après laquelle un événement se produit lorsque la porte est forcée à s'ouvrir. Sélectionnez pour utiliser cette minuterie. Pour l'application serveur, la section Pop-up Snapshot s'ouvre. Si cette fonction est activée, le délai de démarrage de l'activité (voir : **Ajout d'un terminal biométrique**) doit être mis à **0** pour cette porte.

7. Configurer la porte selon les besoins.
8. Cliquer sur **OK**.

8.12. Ajouter des liens de panneau

Les liens de panneau sont des règles qui définissent comment le système doit se comporter lorsque des événements se produisent dans le panneau de contrôle d'accès.

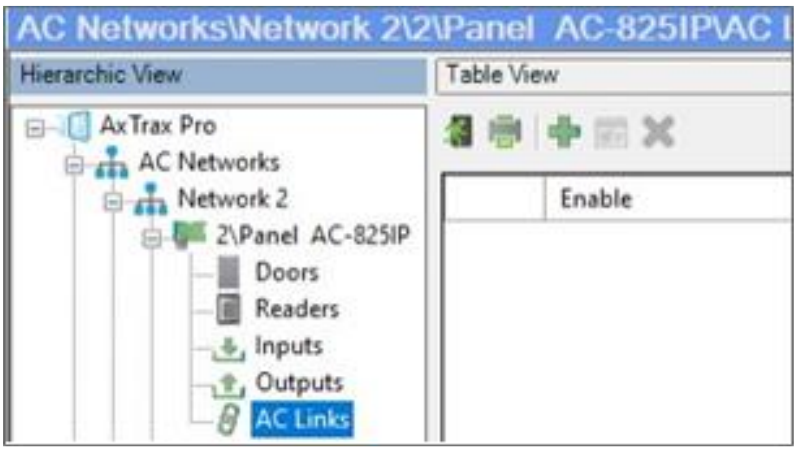
De nombreux événements et **liens** peuvent être définis. Il incombe aux opérateurs d'éviter les définitions contradictoires ou non logiques. Tous les événements qui apparaissent dans la fenêtre des liens ne sont pas activés dans la centrale ; il incombe également à l'opérateur de vérifier ce point. Le fonctionnement des conditions de liaison doit être vérifié après que des modifications ont été apportées aux définitions AC Liens.

La fenêtre du panneau **AC Liens** affiche l'écran suivant:

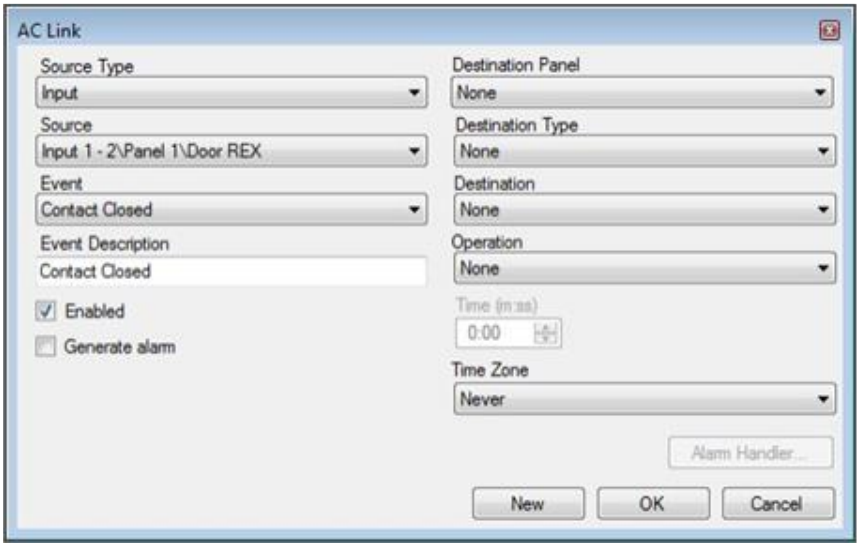
- Un événement sur un panneau et le segment du panneau auquel s'applique la réponse de lien.
- La réponse d'entrée ou de sortie requise.
- Un message d'alarme à afficher sur l'ordinateur AxTraxPro Client..

Pour créer un lien au panneau:

1. Dans l'arborescence, développez l'élément **AC Networks**.
2. Développez le réseau et développez un panneau.
3. Sélectionnez **AC Liens**.



4. Dans la barre d'outils, cliquez sur l'icône 



5. Configurez la règle de lien en fonction des descriptions des champs dans le tableau suivant:

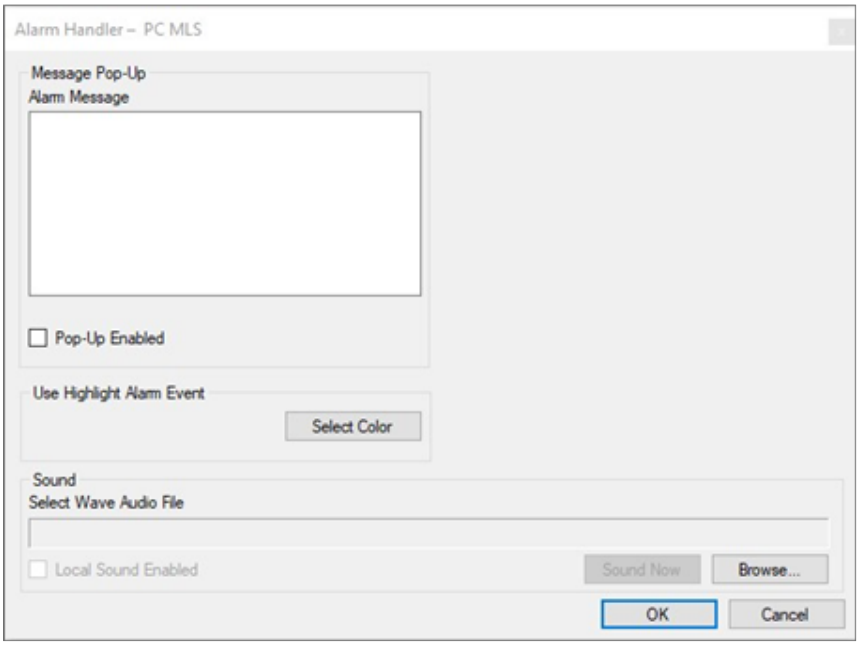
Champs	Description
Type de source	Sélectionnez le type de composant du tableau de bord qui est la source de l'événement: • Entrée • Sortie • Lecteur • Porte • Panneau • Parking de véhicules
Source	Sélectionnez l'élément spécifique du panneau qui appelle l'événement en fonction du type de source sélectionné. Source Dans les panneaux AC-225, AC-425 et AC-825IP, il est possible de créer jusqu'à 8 liens pour chaque type de source. Dans un panneau AC-215, un maximum de 2 liens peut être créé pour chaque type de source

<table>
<tr><th>Champs</th><th>Description</th></tr>
<tr><td>Evénements</td><td>Sélectionnez le type d'événement pour le composant du panneau
<table>
<tr><th>Entrée</th><th>Sortie</th><th>Lecteur</th><th>Porte</th><th>Panneau</th></tr>
<tr>
<td>• Contact Fermer
• Contact Ouvert
• Problème Entrée
• Fonctionnement automatique</td>
<td>• Sortie activé
• Sortie inactive
• Fonctionnement automatique</td>
<td>• Accès autorisé – tous les utilisateurs
• Accès refusé - Tous les codes
• Bouton d'appel
• Sabotage du lecteur
• Accès refusé - Utilisateur sélectionné
• Invalide
• Accès autorisé - utilisateur sélectionné
• Autoprotection du lecteur
• Antipassback temporisé
• Antipassback de porte
• Antipassback global
• Code de contrainte
• Mode carte+carte</td>
<td>• Porte forcée
• Porte laissée ouverte trop longtemps</td>
<td>• Problème d'alimentation en AC
• Batterie faible
• Autoprotection Boîtier
• La batterie n'est pas chargée</td>
</tr>
</table></td></tr>
<tr><td>Description des événements</td><td>Entrez la description du lien ou de l'événement</td></tr>
<tr><td>Activé</td><td>Sélectionnez cette option pour activer la règle de lien</td></tr>
<tr><td>Génère une alarme</td><td>Sélectionnez cette option pour générer un événement d'alarme à côté de l'activité de la règle de lien.</td></tr>
<tr><td>Panneau de destination</td><td>Dans le réseau, sélectionnez le panneau qui doit être déclenché par l'événement de déclenchement de la règle de lien.</td></tr>
<tr><td>Type de destination</td><td>Sélectionnez le composant spécifique du panneau qui doit être déclenché par l'événement de déclenchement de la règle de lien.</td></tr>
<tr><td>Destination</td><td>Sélectionner le composant spécifique du panneau qui doit être déclenché par l'événement de déclenchement de la règle de lien</td></tr>
<tr><td>Fonctionnement</td><td>Sélectionner l'opération à effectuer par le composant de panneau de destination</td></tr>
<tr><td>Durée de l'opération</td><td>Définir une durée pour l'opération. Cette case n'est disponible que lorsqu'une opération basée sur le temps est sélectionnée.</td></tr>
</table>

Délai avant l'opération de destination	Sélectionnez le délai (en secondes) de l'opération. Cette option apparaît lorsque le **type de destination** est spécifié.
Fuseau horaire	Sélectionnez le fuseau horaire auquel la règle de lien s'applique
Gestionnaire d'alarme	La fonction Administrateur d'alarmes n'est activée que lorsque l'option **Générer une alarme** est sélectionnée. La fenêtre de configuration de l'administrateur d'alarme contient les champs suivants • **Alarm Message (Message d'alarme) :** Tapez un message personnel qui s'affichera à l'écran comme message d'alarme lorsque l'événement sélectionné se produit**.** • **Pop-up Enabled (Fenêtre contextuelle activée) :** Sélectionnez cette option pour activer un message d'alarme contextuel. • **Bouton de sélection couleur:** Une fenêtre de sélection des couleurs s'ouvre et permet de choisir la couleur du message d'alarme. • **Bouton Parcourir... :** permet de rechercher et de télécharger un fichier audio wav qui émettra un son lorsque l'événement sélectionné se produira**.** • **Bouton Sonner maintenant :** Après avoir téléchargé le fichier audio, cliquez sur le bouton pour l'écouter. • **Local Sound Enabled (Son local activé) :** Sélectionnez cette option pour activer le son de l'alarme. • **Entrée alarme incendie**: permet d'ouvrir toutes les sorties, ce qui est généralement le cas pour les alarmes incendie. En outre, lorsqu'une caméra est connectée à un panneau, les champs suivants apparaissent dans la fenêtre • **Caméra :** Liste des caméras disponibles**.** • **Options :** Quelle alarme est déclenchée**.** • **Opus activé :** Active une fenêtre contextuelle qui s'affiche sur l'écran de l'utilisateur lorsque l'alarme est déclenchée. • **Options de fermeture de la fenêtre :** Peut être sélectionnée "**Par minuterie**" et l'heure spécifiée, ou manuellement.

6. [Optionnel] Définition d'une alarme générale:
   a. Sélectionnez “**Generate Alarm”** pour activer le bouton **Alarm Handler** (Gestionnaire d'alarme)..

b. Cliquer sur **Alarm Handler**



   c. Configurez le gestionnaire d'alarme selon les besoins.
   d. Cliquez sur **OK** pour revenir à la fenêtre de **lien.**

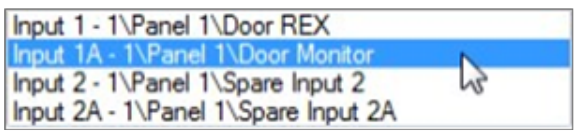
7. Cliquer sur **OK**.

8.12.1. Déclenchement global de groupes de sorties

Le déclenchement global est utilisé pour les activations entre panneaux. Par exemple, lors d'une alarme incendie, toutes les portes du système sont ouvertes à partir d'une seule entrée.

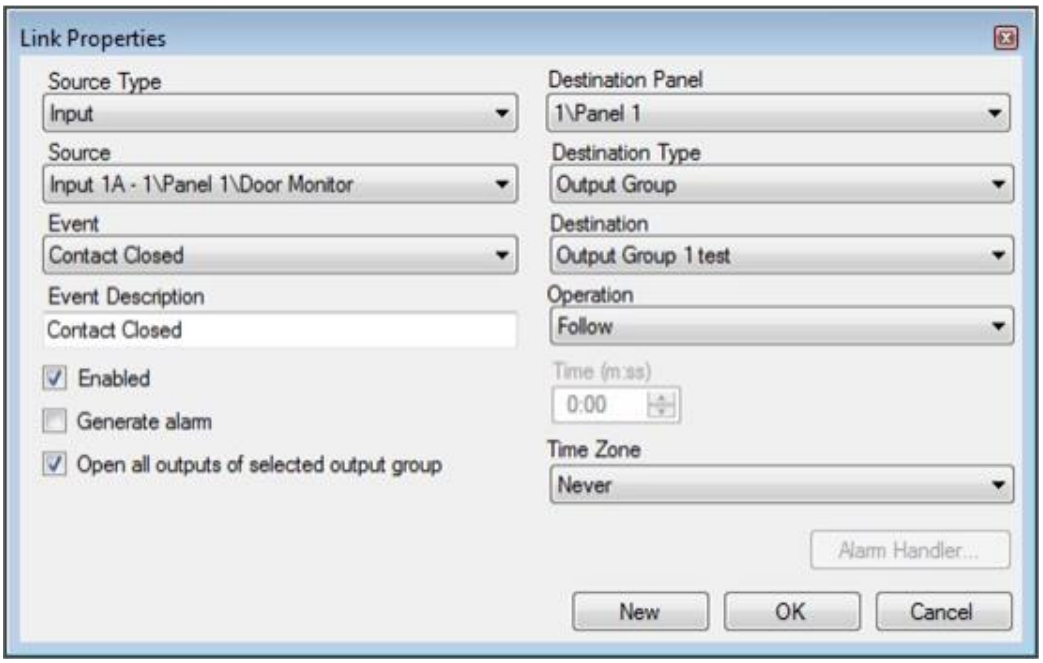
Pour créer un déclenchement global de groupes de sorties:

1. Dans l'arborescence, développez l'élément **AC Networks** (Réseaux CA).
2. Vouw een netwerk uit en vouw een paneel uit.
3. Sélectionnez **AC Lien**.
4. Dans la barre d'outils, cliquez sur l'icône 
5. Développez un réseau et un panneau:
   a. Dans **Source Type**, sélectionnez **Input**.
   b. Dans **Source**, sélectionnez soit un **Door Monitor**, soit une entrée libre.



   c. Dans **Destination Panel**, sélectionnez le panneau approprié.
   d. Dans **Destination Type**, sélectionnez **Output Group**.

e. Sélectionnez **Open all outputs of selected output group**, qui sont maintenant visibles.



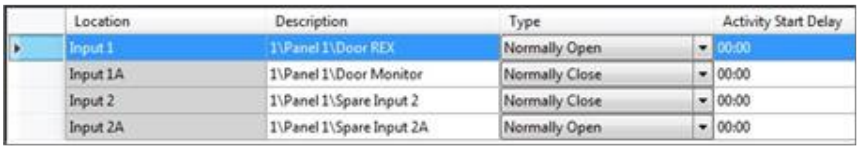
8.13. Configuration des entrées

Chaque panneau dispose de quatre entrées. La carte d'extension MD-IO84 ajoute huit entrées supplémentaires (soit un total de 12 entrées). La carte d'extension MD-D02 ou MD-D04 ajoute quatre entrées (soit un total de 8 entrées). Certaines entrées sont spécifiques et ont une fonction standard, d'autres sont d'usage général.

La fenêtre du tableau montre les paramètres de chaque entrée. Le type d'entrée est programmé séparément, qu'il s'agisse d'une entrée spécifique ou d'une entrée à usage général.

Pour configurer une entrée:

1. Dans **l'arborescence**, développez l'élément **AC Networks**.
2. Développez un réseau et un panneau.
3. Sélectionnez **Inputs**



Location	Description	Type	Activity Start Delay
Input 1	1\Panel 1\Door REX	Normally Open	00:00
Input 1A	1\Panel 1\Door Monitor	Normally Close	00:00
Input 2	1\Panel 1\Spare Input 2	Normally Close	00:00
Input 2A	1\Panel 1\Spare Input 2A	Normally Open	00:00

4. Définissez les propriétés conformément aux descriptions des champs dans le tableau suivant:
5. Sélectionnez le type d'entrée à surveiller comme indiqué ci-dessous.

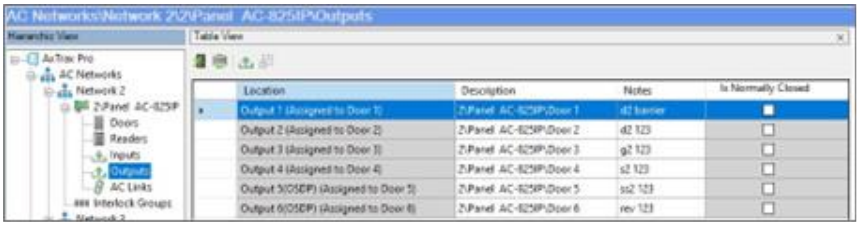
Champs	Description
Type	électionnez le type d'entrée à surveiller. • **Normalement ouverte/fermée :** Une entrée dans un état ouvert ou fermé. • **Normalement ouverte/fermée 1 résistance :** une entrée à l'état ouvert, fermé ou problème. Cette option n'est disponible que pour les entrées surveillées. • **Normalement ouverte/fermée 2 Résistances :** Une entrée dans un état ouvert, fermé ou Problème, avec des contrôles supplémentaires de court-circuit et de sabotage de circuit ouvert. Cette option n'est disponible que pour les entrées surveillées. Pour plus d'informations, consultez le manuel d'installation du panneau concerné.

8.14. Commande manuelle des sorties

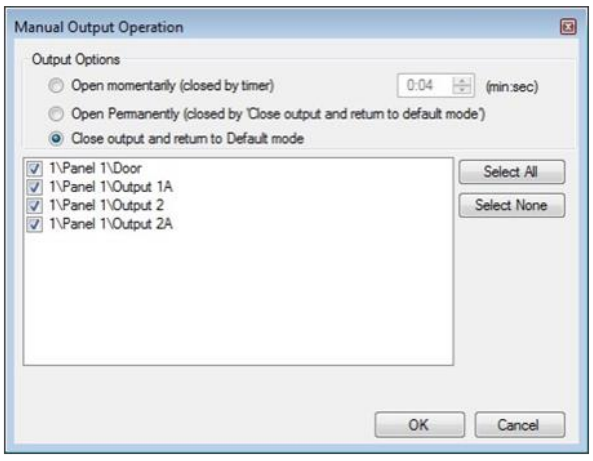
La fenêtre Commande manuelle des sorties permet à un opérateur d'ouvrir ou de fermer directement un groupe de sorties sélectionnées sur un panneau.

Pour ouvrir ou fermer manuellement une sortie:

1. Dans **l'arborescence**, développez l'élément **AC Networks** et développez un réseau.
2. Sélectionnez un panneau.



3. Dans la barre d'outils, cliquez sur l'icône 



4. Sélectionnez une option:

   - **Temporarily Open (Ouverture temporaire) -** Ouvre toutes les sorties sélectionnées pour la durée définie dans la période.
   - **Ouverture permanente -** Ouvre toutes les sorties sélectionnées.
   - **Close output and return to default mode (Fermer la sortie et revenir au mode par défaut) -** Ferme les sorties sélectionnées et ramène la commande au mode par défaut.

5. Cochez les cases des sorties auxquelles l'opération doit être appliquée.
6. Cliquer sur **OK**.

9. Gestion des groupes

Vous pouvez créer des groupes d'accès et des zones, ainsi que des groupes d'entrée et de sortie utilisés par le système pour créer des règles automatiques.

9.1. Ajouter des groupes d'accès

Un groupe d'accès contient une liste de lecteurs de porte et les zones horaires dans lesquelles chacun est disponible pour l'accès. Chaque utilisateur est assigné à un groupe d'accès.

Pour ajouter un groupe d'accès:

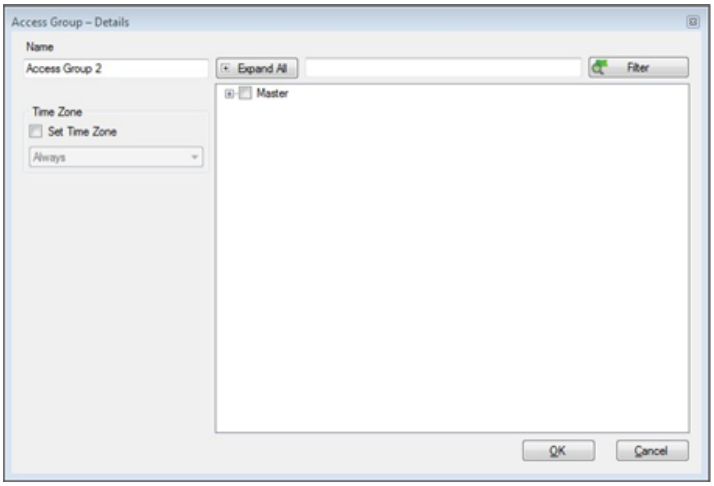
1. Dans l'arborescence, développez l'élément **Groupes.**
2. Sélectionnez “**Access Groups”**.

Dans la barre d'outils, cliquez sur l'icône 

4. Dans le champ **Description**, entrez le nom du groupe d'accès et cliquez sur **OK**.

Le nouveau groupe d'accès apparaît dans **l'arborescence.**

3. Sélectionnez le groupe d'accès dans l'arborescence et cliquez sur l'icône 



6. Cochez la case "**Définir le fuseau horaire**".

   Sélectionnez une heure dans le menu déroulant "**Time Zone**".

7. Développez la liste et sélectionnez les lecteurs souhaités.

9. Cliquer sur **OK**.

   La fenêtre se ferme et le nouveau groupe d'accès apparaît dans la zone d'affichage.

9.2. Ajouter des zones d'accès

Un grand site peut être divisé en plusieurs zones d'accès plus petites et plus faciles à gérer. Des rapports distincts peuvent être créés pour chaque zone. En outre, des règles globales d'anti-passback peuvent être appliquées à chaque zone d'accès. Lorsque les règles globales d'anti-passback sont en vigueur, les utilisateurs ne peuvent pas entrer à nouveau dans une zone d'accès tant qu'ils ne l'ont pas quittée.

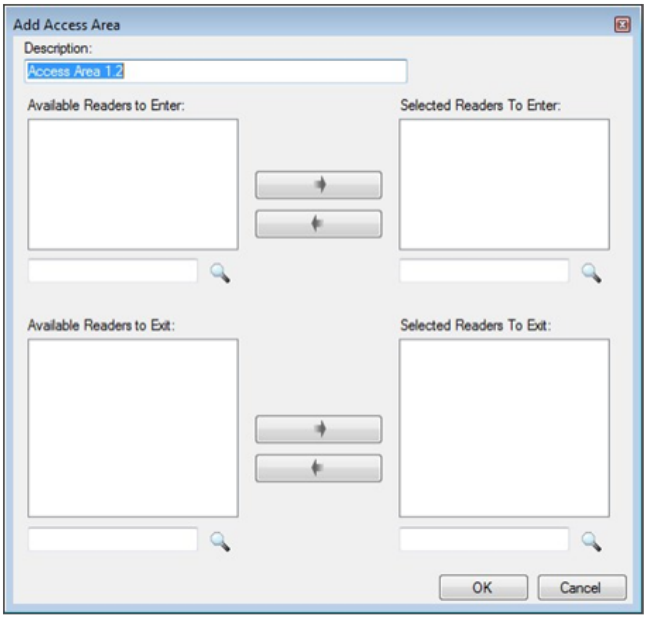
La fenêtre **Zone d'accès** permet d'ajouter des lecteurs d'entrée et de sortie à une zone de cette installation..

Pour ajouter une zone d'accès:

1. Dans **l'arborescence**, développez l'élément **Groupes**.

2. Développez l'élément **Zones d'accès** et cliquez sur **Global.**

3. Dans la barre d'outils, cliquez sur l'icône 



4. Dans le champ **Description**, entrez un nom pour la **zone d'accès**.
5. Sélectionnez et déplacez les lecteurs souhaités de ‘’**Available Readers to Enter’’** vers ‘’**Selected readers to Enter**’’, à l’aide des flèches.
6. Sélectionnez et déplacez les lecteurs souhaités de ‘’**Available Readers to Exit’’** vers ‘’**Selected Readers to Exit’’,** à l’aide des flèches.
7. Cliquer sur **OK**.

   La fenêtre se ferme et les nouvelles zones d'accès apparaissent dans la **zone d'affichage**.

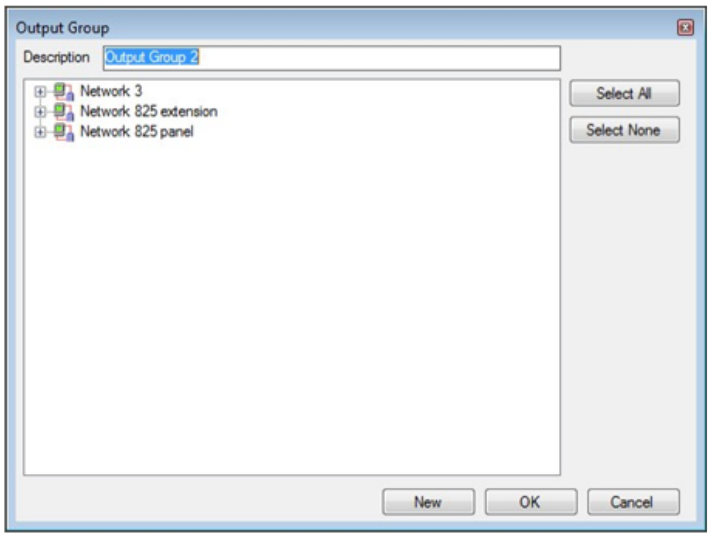
9.3. Ajouter des groupes de sorties

Les groupes de sortie sont une collection de sorties de panneau qui peuvent être utilisées dans les liens de panneau pour effectuer des opérations avancées, telles que le contrôle de l'ascenseur.

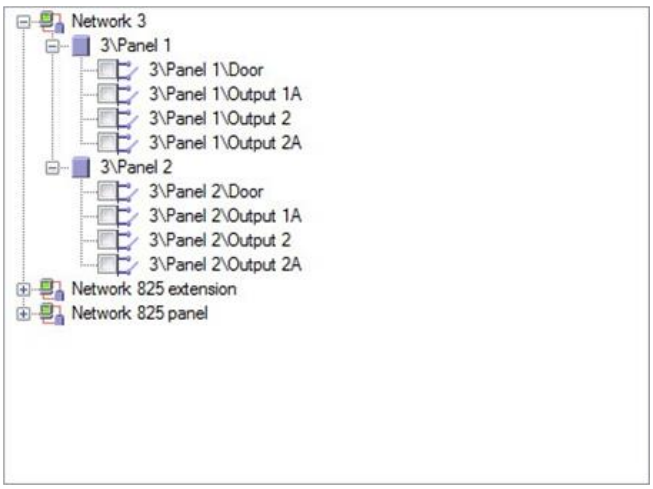
Pour ajouter un groupe de sorties:

1. Dans **l'arborescence**, développez l'élément **Groupes.**
2. Sélectionnez **Outputs Groups**.

   Dans la barre d'outils, cliquez sur l'icône 



4. Dans le champ **Description**, saisissez un nom pour le groupe de sortie.
4. Développez un réseau pour afficher ses panneaux.



5. Cochez les cases des sorties correspondantes. Vous pouvez également utiliser l'option "**Select All**".
7. Cliquer sur **OK**.

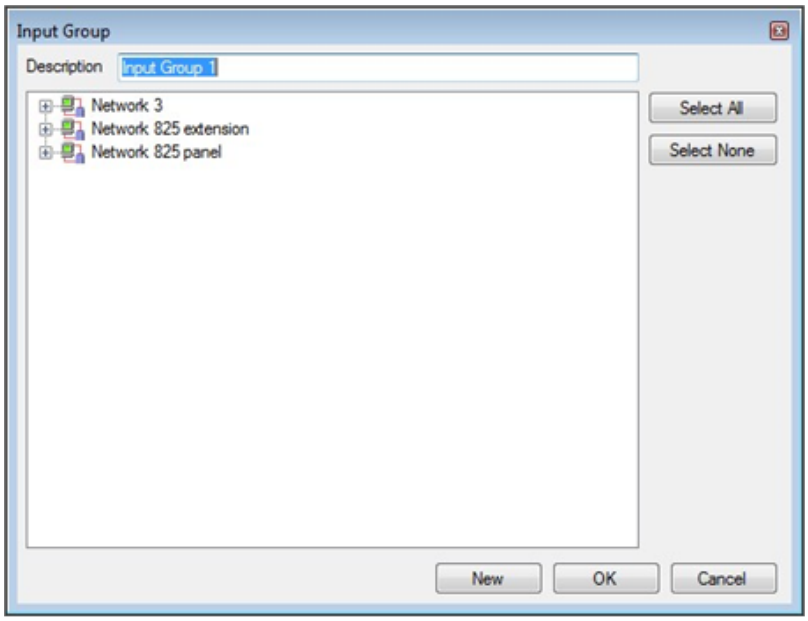
   La fenêtre se ferme et le nouveau groupe de sorties apparaît dans la zone d'affichage.

9.4. Ajouter des groupes d'entrée

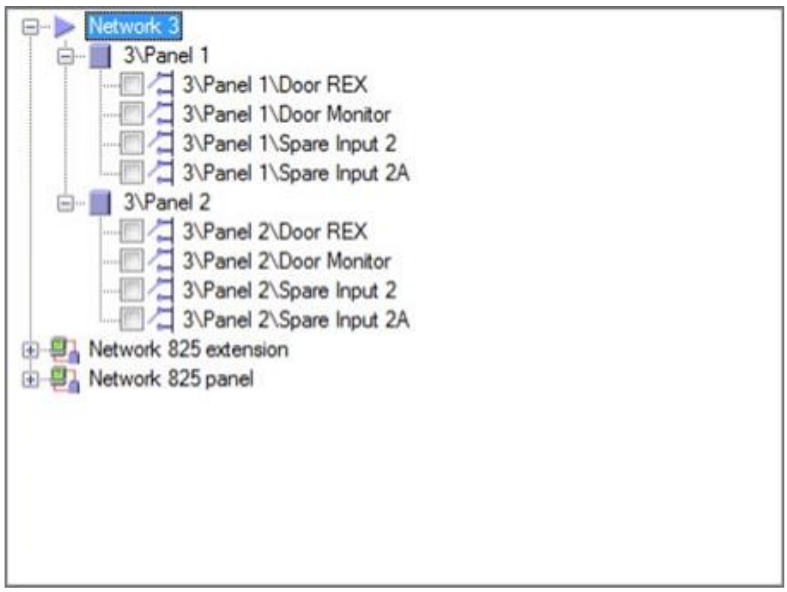
Les groupes d'entrées sont une collection d'entrées provenant d'un ou de plusieurs panneaux qui peuvent être utilisées dans les liens entre panneaux pour effectuer des opérations avancées.

Pour créer un groupe d'entrées:

1. Dans l'arborescence, développez l'élément **Groupes**.
2. Sélectionnez **Input Group.**
3. Dans la barre d'outils, cliquez sur l'icône 



4. Dans le champ **Description**, saisissez le nom du **groupe d'entrée**.
5. Développez un réseau pour afficher ses panneaux.



6. Cochez les cases de toutes les entrées pertinentes. Vous pouvez également utiliser l'option **Sélectionner tout**.
7. Cliquez sur **OK.**

   La fenêtre se ferme et le nouveau groupe d'entrée apparaît dans la zone d'affichage.

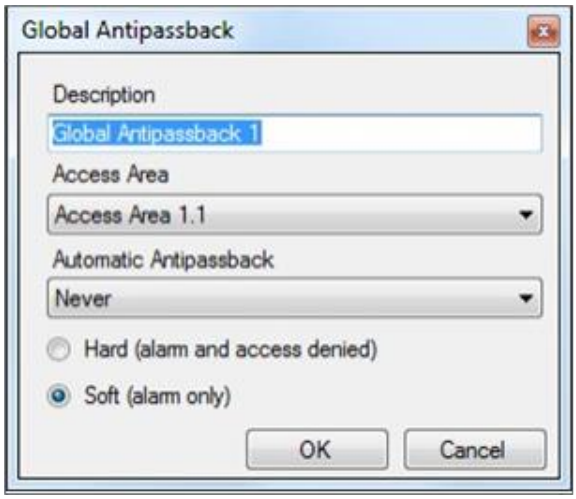
9.5. Ajouter des règles d'anti-passback global

La fonctionnalité Antipassback global est exécutée uniquement lorsque le serveur AxTraxPro est connecté et qu'il contrôle l'ensemble du système de contrôle d'accès.

> Une règle globale d'Antipassback ne peut être ajoutée que si une zone d'accès a été définie (voir Adding Access Areas).

Pour créer des règles d'anti-passback:

1. Dans l'arborescence, cliquez sur **Global Antipassback**.
2. Dans la barre d'outils, cliquez sur l'icône 



3. Dans le champ **Description**, saisissez un nom pour la règle Antipassback.
4. Dans le menu déroulant **Zone d'accès**, sélectionnez la zone d'accès appropriée..
5. Dans le menu déroulant **Automatic Antipassback**, sélectionnez le fuseau horaire auquel s'applique l'Antipassback global.
6. Sélectionnez l'option **Hard** ou **Soft** Antipassback..
7. Cliquez sur **OK**.

   La fenêtre se ferme et la règle Global Antipassback apparaît dans la zone d'affichage.

L'Antipassback global applique un événement Antipassback uniquement aux lecteurs "Entrée" de la "Zone" définie".

Pour appliquer l'Antipassback également aux lecteurs de sortie, définissez une nouvelle zone avec des sens de lecture opposés:

Les lecteurs définis comme "lecteurs d'entrée" dans la première zone doivent être redéfinis comme lecteurs de sortie dans la nouvelle zone, et les lecteurs de sortie de la première zone doivent être définis comme "lecteurs d'entrée" dans la deuxième zone.

9.6. Gestion de Lockdown

9.6.1. Ajouter des groupes de lockdown

Un groupe de fermeture (Lockdown) contient une liste des portes verrouillées et des opérateurs qui gèrent et contrôlent la fermeture (Lockdown).

Pendant une fermeture, les portes du groupe de fermeture ne peuvent être ouvertes que par des utilisateurs autorisés.

Un lockdown ne peut avoir lieu que si le serveur AxTraxPro est connecté et contrôle l'ensemble du système de contrôle d'accès.

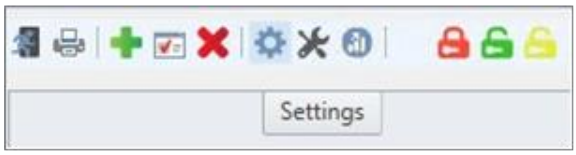
Une opération lockdown ne peut être utilisée qu'avec les panneaux AC-825IP.

Le réseau AC-825IP doit être spécifié avant qu'un groupe lockdown puisse être ajouté.

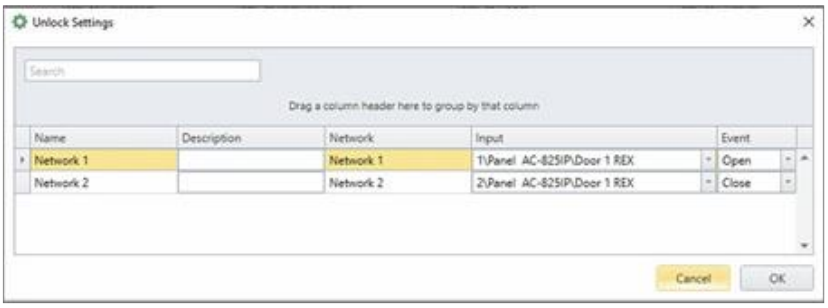
Configuration de l'entrée du réseau AC-825IP:

Chaque réseau AC-825IP en lockdown doit disposer d'une entrée dédiée permettant la désactivation manuelle d'un lockdown actif.

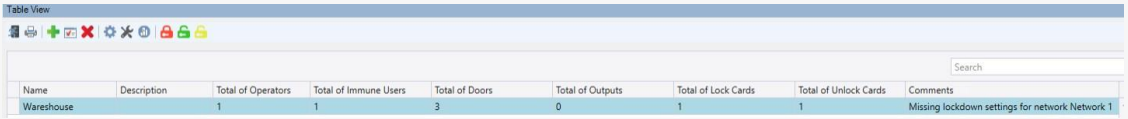
1. Dans la table, sélectionnez l'icône Settings (Paramètres) dans la barre d'outils.



2. Sélectionnez un **réseau**, une **entrée** et un **événement** pour les paramètres de déverrouillage physique..

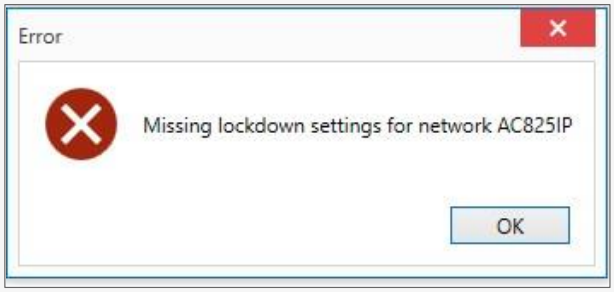


Une entrée doit être sélectionnée avant de pouvoir configurer le groupe lockdown. Si une entrée n'est pas sélectionnée, le groupe ne peut pas être activé.



3. Cliquer sur **OK**.

Le message suivant s'affiche si les paramètres réseau de l'AC-825IP ne sont pas configurés.

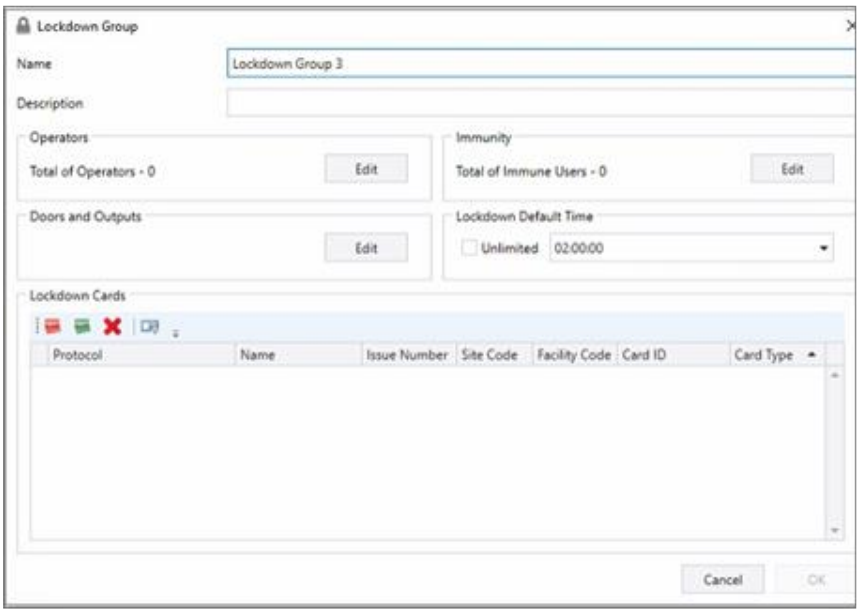


Le message suivant s'affiche si les paramètres réseau de l'AC-825IP ne sont pas configurés.

9.6.1.1. Ajouter un groupe Lockdown dans l'arborescence

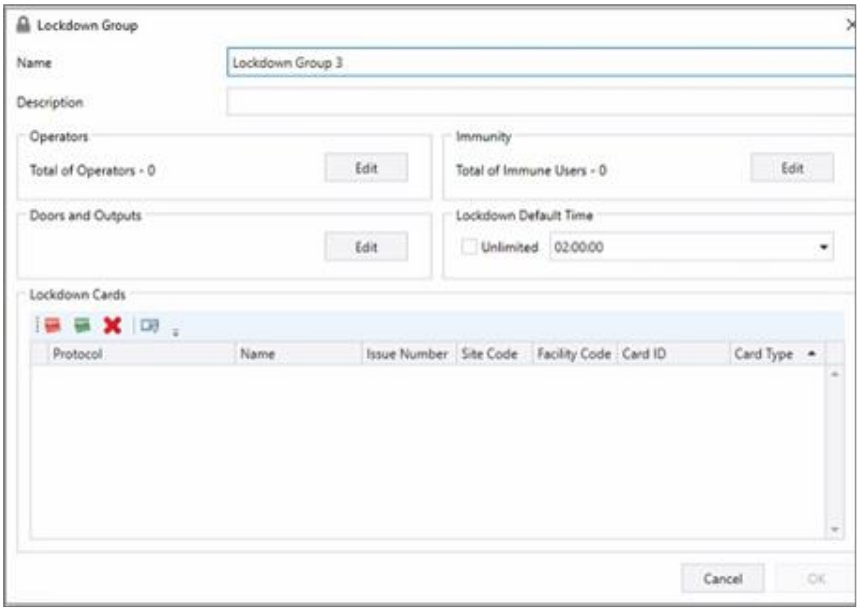
Ajouter un groupe Lockdown:

1. Dans l'arborescence, développez l'élément **Groupes**.
2. Sélectionnez **Lockdown Group**.
3. Dans la barre d'outils, cliquez sur l'icône 



4. Entrez un nom et une description pour le groupe Lockdown dans les champs appropriés.
5. Pour ajouter des opérateurs au groupe, voir Add/Edit Operators within Lockdown Group.
6. Pour ajouter des portes et des sorties au groupe, voir Add/Edit Doors and Outputs within Lockdown Group.
7. Pour ajouter des utilisateurs d'immunité au groupe, voir Add/Edit Immunity Users within Lockdown Group.
8. Pour ajouter une nouvelle carte lockdown au groupe, voir Add New Lock or Release Card to Lockdown Group.
9. Pour ajouter une carte lockdown existante au groupe, voir Add Existing Lockdown Card to Lockdown Group.

10. Pour ajouter l'heure de lockdown, tapez ou sélectionnez l'heure dans **Lockdown Default Time**.



Les paramètres de lockdown par défaut sont les suivants

- Opérateurs - 0
- Utilisateurs avec immunité - 0
- Heure de lockdown par défaut - 2:00 heures

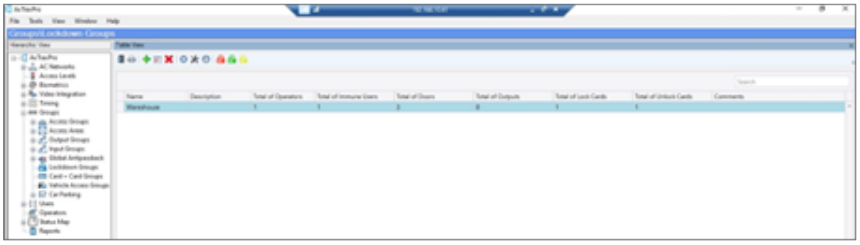
11. Cliquer sur **OK**.

    Le nouveau groupe Lockdown apparaît dans la vue en tableau.

9.6.1.2. Modification des propriétés d'un groupe Lockdown

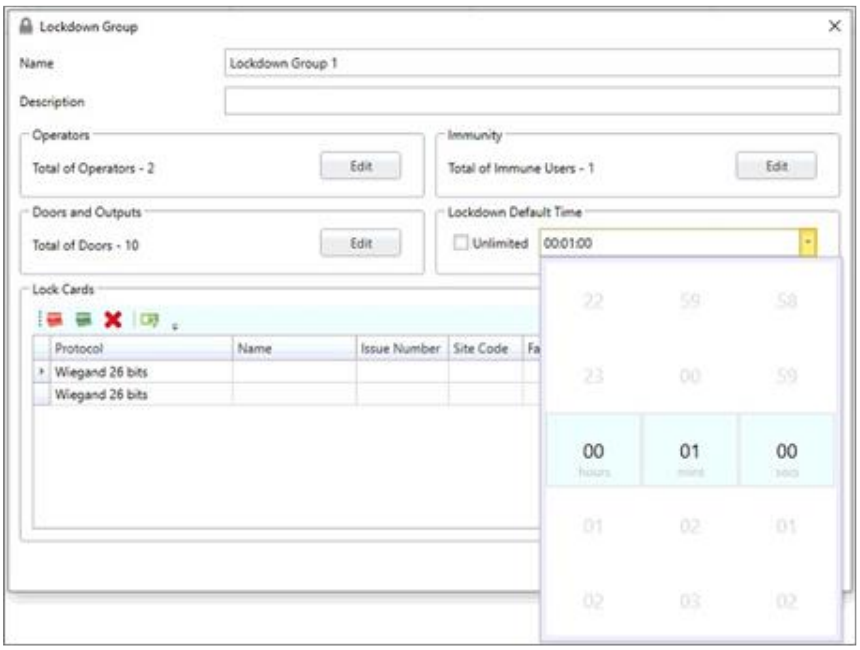
Pour modifier les propriétés d'un groupe Lockdown, procédez comme suit:

1. Dans la vue de table, sélectionnez le groupe Lockdown à modifier.



2. Sélectionnez  (Éditer Groupe) dans la barre de menu.
3. Si nécessaire, modifiez **le nom** ou la **description** du groupe..
4. Le nombre d'opérateurs définis dans le groupe s'affiche. Pour modifier, cliquez sur **Modifier** (voir Add/Edit Operators within Lockdown Group).
5. Le nombre de portes et sorties définies dans le groupe s'affiche. Pour modifier, cliquez sur **Modifier** (voir Add/Edit Doors and Outputs within Lockdown Group).
6. Le nombre d'utilisateurs immuns définis dans le groupe s'affiche. Pour le modifier, cliquez sur **Modifier** (voir Add/Edit Immunity Users within Lockdown Group).
7. Les cartes lockdown définies dans le groupe s'affichent. Pour ajouter une nouvelle carte Lockdown au groupe, (voir Add New Lock or Release Card to Lockdown Group).
8. Pour ajouter une carte Lockdown existante au groupe, (voir Add Existing Lockdown Card to Lockdown Group).

9. Pour modifier l'heure de Lockdown, tapez ou sélectionnez l'heure dans **Lockdown Default Time** (Heure de verrouillage par défaut)..



10. Cliquer sur **OK.**

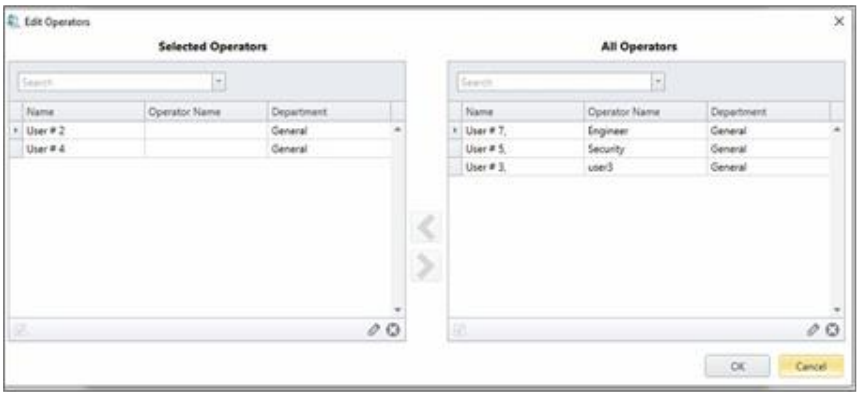
9.6.1.3. Ajouter/modifier des opérateurs dans un groupe lockdown

Pour ajouter/modifier des opérateurs dans un groupe lockdown:

Seuls les opérateurs ayant des droits de lecture/modification sur le Lockdown peuvent être ajoutés.

1. Dans la fenêtre des propriétés du groupe, cliquez sur "**Edit''** dans **Opérateurs.**

2. Pour ajouter des opérateurs au groupe, sélectionnez les opérateurs souhaités dans le tableau de droite et cliquez sur la flèche du haut pour les déplacer dans la liste de gauche. Pour supprimer des opérateurs, faites l'inverse.

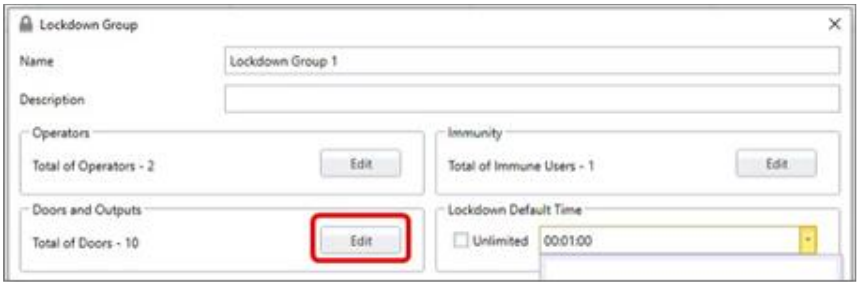


3. Après avoir effectué toutes les modifications, cliquez sur **OK**.

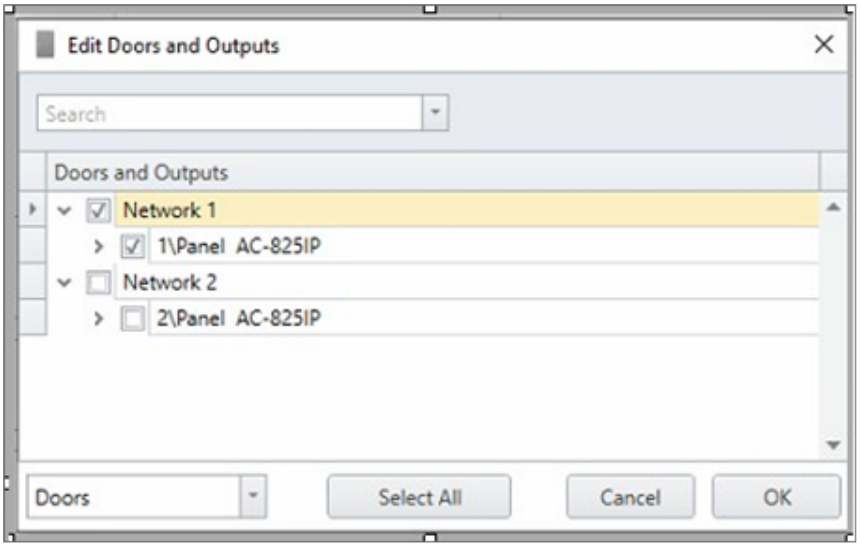
9.6.1.4. Ajouter/modifier des portes et des sorties dans le groupe Lockdown

Pour ajouter/modifier des portes et des sorties dans le groupe Lockdown:

1. Dans la fenêtre des propriétés du groupe, cliquez sur **Edit** dans **Doors and Outputs**.



2. Pour modifier la sélection des portes, sélectionnez **Portes**. Pour modifier la sélection des sorties, sélectionnez **Sorties**. Cocher/décocher les portes ou les sorties à ajouter/supprimer du groupe.



3. Cliquez sur OK après avoir effectué toutes les modifications.

9.6.1.5. Ajouter/modifier des utilisateurs avec immunité dans le groupe lockdown

Les utilisateurs bénéficiant d'une immunité sont les utilisateurs qui peuvent ouvrir les portes lors d'une Lockdown.

> Une liste d'utilisateurs bénéficiant d'une immunité doit être sélectionnée séparément pour chaque groupe de Lockdown. Il n'y a pas d'immunité globale pour les groupes lockdown.

Pour ajouter/modifier des utilisateurs bénéficiant d'une immunité au sein d'un groupe de Lockdown, procédez comme suit:

1. Dans la fenêtre Propriétés du groupe, cliquez sur **Modifier** sous **Immunité**.

2. Pour ajouter des utilisateurs avec immunité, sélectionnez les utilisateurs souhaités dans le tableau de droite et cliquez sur la flèche du haut pour les déplacer dans la liste de gauche. Pour supprimer des utilisateurs, faites l'inverse.
3. Une fois toutes les modifications effectuées, cliquez sur **OK**.

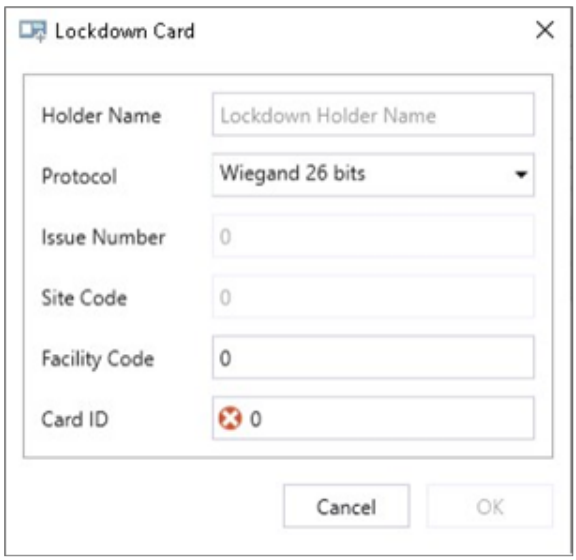
9.6.1.6. Ajouter une nouvelle carte de verrouillage ou de validation au groupe Lockdown

Vous devez définir au moins deux cartes lockdown. Une carte lockdown déclenche un lockdown et l'autre carte lockdown libère un lockdown. Les cartes doivent être conservées en lieu sûr pour une utilisation en cas d'urgence. Une carte lockdown peut être partagée par plusieurs utilisateurs.

Pour ajouter une nouvelle carte lockdown à un groupe de lockdown:

Vous ne pouvez pas utiliser une carte existante dans le système pour créer une nouvelle carte de blocage/libération.

1. Pour ajouter de nouvelles cartes lockdown au groupe, sélectionnez pour une carte lockdown ou pour une carte de libération



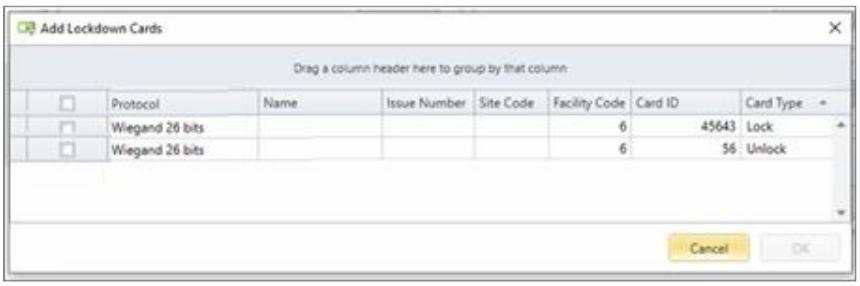
2. Pour chaque nouvelle carte lockdown à ajouter, saisissez la configuration requise pour la carte dans les champs suivants:
   - Nom (Holder name)
   - Protocole(Protocol)
   - numéro de délivrance (Issue Number)
   - Site Code
   - Facility Code
   - ID de la carte (Card ID)

3. Après avoir effectué toutes les modifications, cliquez sur **OK**.

9.6.1.7. Ajouter une carte lockdown existante à un groupe de lockdown

Pour ajouter une carte Lockdown existante à un groupe de lockdown, procédez comme suit:

1. Pour ajouter une carte Lockdown existante au groupe, cliquez sur l'icône dans la barre d'outils.
   La fenêtre Ajouter une carte Lockdown affiche les cartes existantes.



2. Sélectionnez les cartes à ajouter au groupe lockdown et cliquez sur **OK**.

9.6.2. Utilisation des groupes lockdown

Les opérations des groupes lockdown peuvent être contrôlées de la manière suivante:

1. En utilisant des cartes d'accès spécialement configurées pour verrouiller ou déverrouiller un système de fermeture.

> Un lockdown peut être initié par une carte lockdown ou par le client du logiciel de gestion AxTraxPro sur tous les lecteurs du système.

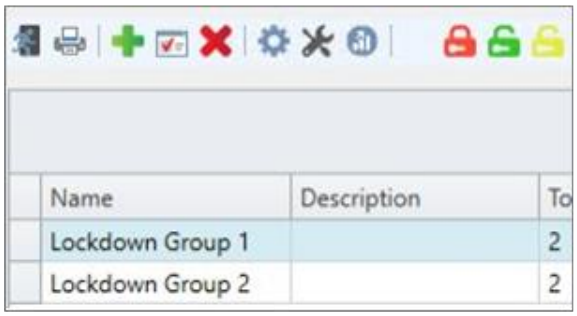
> Chaque fois qu'une carte lockdown initie un lockdown, la minuterie de lockdown est réinitialisée et recommence à compter. Le temps de verrouillage par défaut est de 2 heures.

> Pendant une Lockdown, les portes et sorties spécifiées dans la Lockdown ne peuvent être ouvertes que par des utilisateurs autorisés, à partir d'un contournement de la Lockdown ou par un opérateur autorisé.

1. Utilisation du logiciel de gestion AxTraxPro.

Démarrage du lockdown manuel à l'aide du logiciel de gestion AxTraxPro:

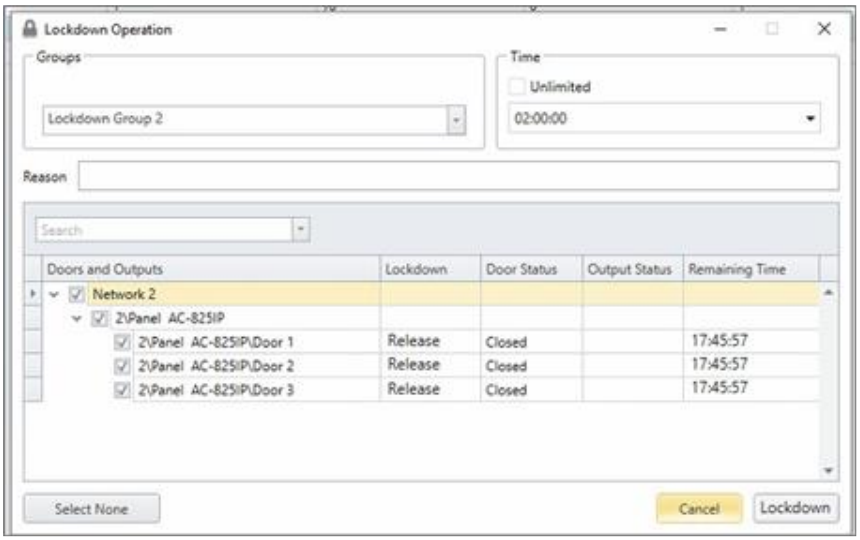
1 Dans la vue tableau, sélectionnez le groupe Lockdown souhaité.



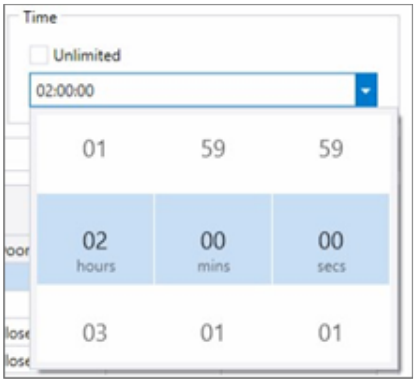
Si un groupe "lockdown" n'est pas représenté par une couleur, le groupe "lockdown" est ouvert.

2. Cliquez sur l'icône Groupe Lockdown

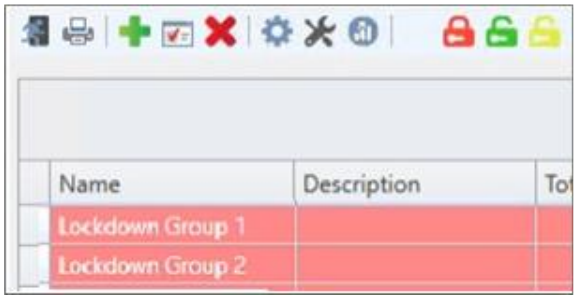
3. Cochez/décochez les portes qui doivent être verrouillées.



4. Pour définir la durée de verrouillage (Lockdown), décochez la case **Temps(Time**) à côté de **Illimité (Unlimited**) et sélectionnez la durée.



5. Cliquer sur **Lockdown**.

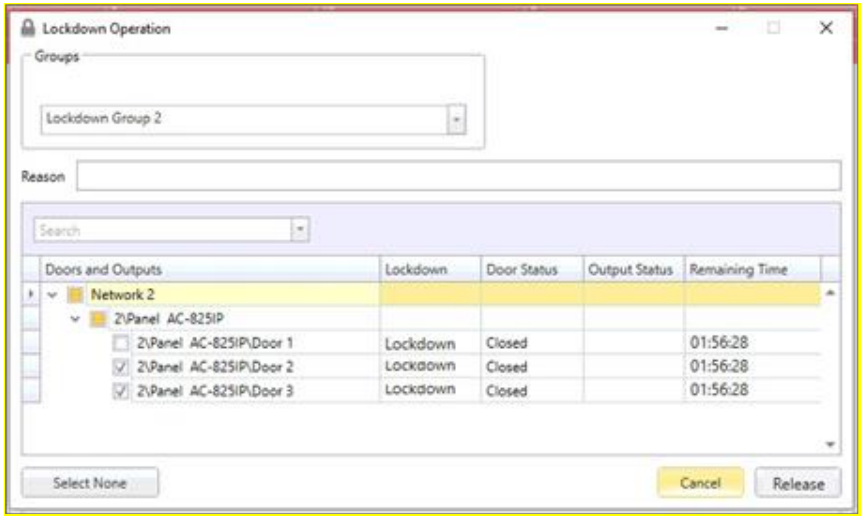


Lorsqu'un groupe lockdown est surligné en rouge, toutes les portes du groupe de lockdown sont verrouillées.

Désactiver un verrouillage (Lockdown) et libérer la ou les portes spécifiées à l'aide du logiciel de gestion AxTraxPro:

1. Dans la vue tableau, sélectionnez le groupe de verrouillage (Lockdown) souhaité et cliquez sur l'icône **Release Group**.

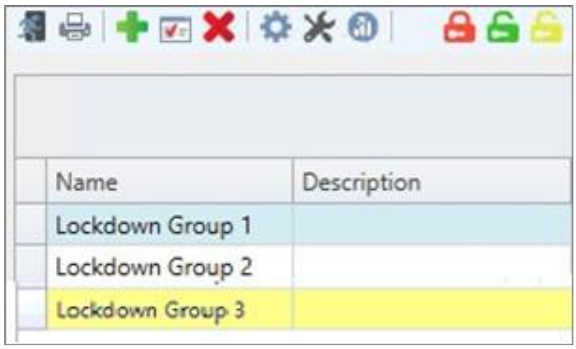
2. Cochez/décochez les portes qui doivent être ouvertes.



3. Cliquez sur **Release** (Déverrouiller).
4. Cliquez sur **Release** (Déverrouiller) pour supprimer le lockdown.

ou

5. Cliquez sur **No**n pour annuler le Lockdown .

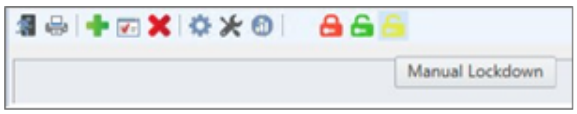


Lorsqu'un groupe lockdown est marqué en jaune, seule une partie des portes du groupe de lockdown est verrouillée.

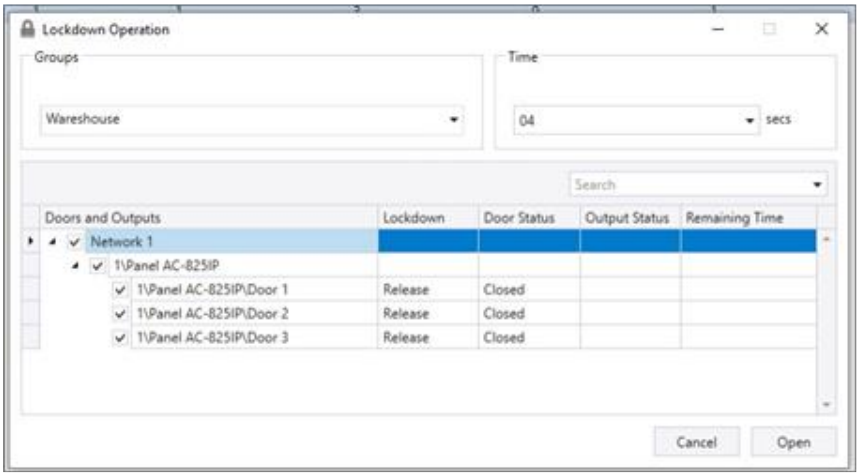
Pour contourner manuellement un lockdown pour une période spécifiée et pour une porte particulière, uniquement avec le logiciel de gestion AxTraxPro:

Cette étape permet aux utilisateurs ayant des droits d'accès autorisés d'ouvrir une porte et sortier.

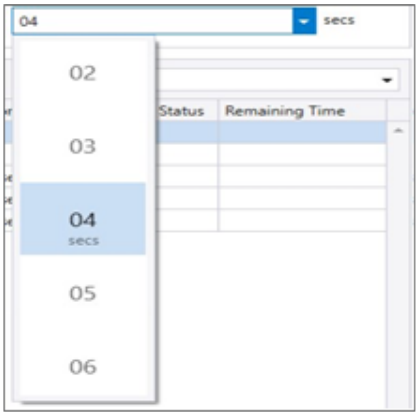
Dans la vue tableau, sélectionnez le groupe Lockdown souhaité et cliquez sur l'icône **Manual Lockdown**.



2. Cochez/décochez la porte à ouvrir.



3. Tapez ou sélectionnez l'heure.

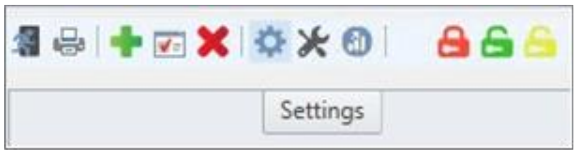


La valeur du temps est exprimée en secondes..

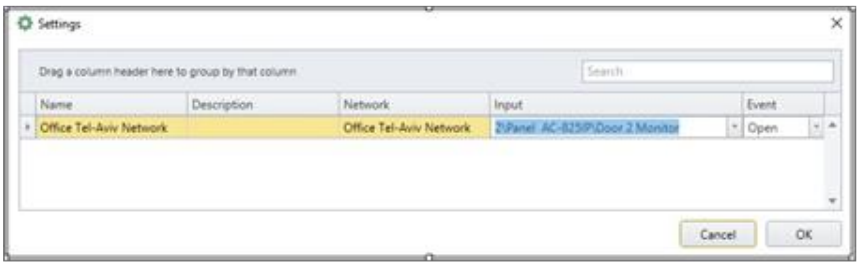
4. Cliquer sur **Open (Ouvrir)**.

Pour définir un événement qui déclenche automatiquement le lockdown:

1. Dans la vue en tableau, sélectionnez le groupe Lockdown souhaité et cliquez sur l'icône (Settings) Paramètres dans la barre d'outils..



2. Sélectionnez l'**entrée** et **l'événement** qui déclenchent le Lockdown pour ce groupe..

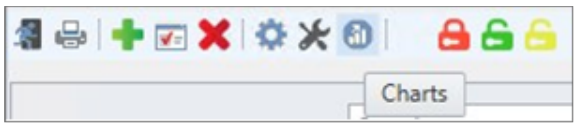


3. Cliquer sur **OK**.

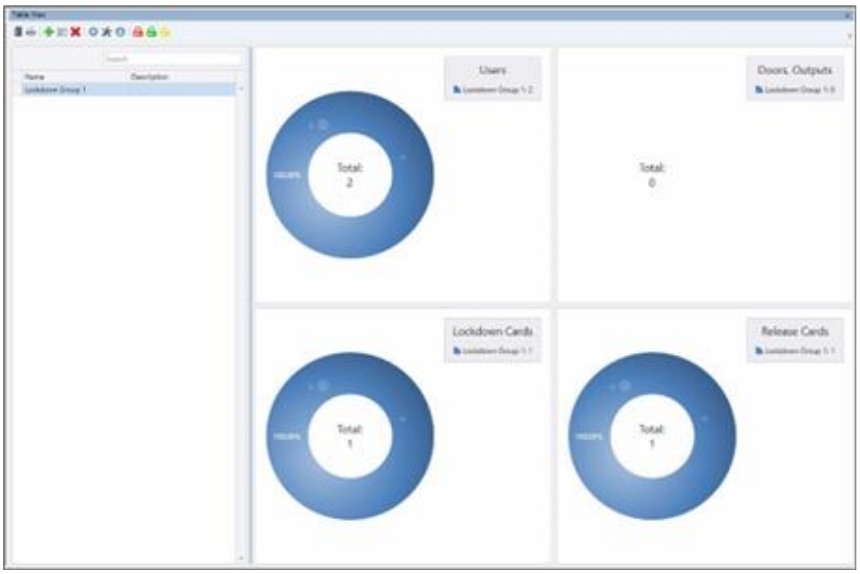
Chaque réseau AC-825IP doit avoir des entrées de (Lockdown) verrouillage spécifiques.

Pour afficher un graphique de Lockdown:

1. Cliquez sur l'icône **Charts** (Graphiques).

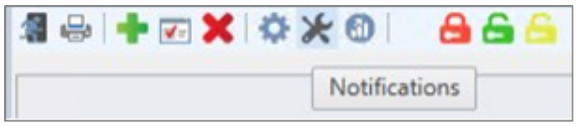


2. Pour fermer le graphique (Chart), cliquez sur l'icône 

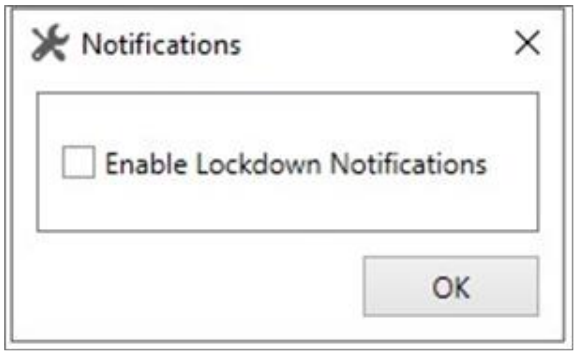


Pour recevoir une notification concernant un Lockdown:

1. Cliquez sur l'icône  **Notifications.**



2. Cochez la case "**Enable Lockdown Notifications"**.



3. Cliquer sur **OK**.

9.7. Définition des groupes Carte + Carte

Le mode Carte + Carte est un mode sécurisé qui nécessite deux titulaires de carte (utilisateurs) pour accorder l'accès à un lecteur spécifique.

Cette fonction n'est pas disponible pour les panneaux de contrôle d'accès AC-215.

9.7.1. Ajouter un groupe Carte + Carte

Vous devez d'abord créer un groupe Carte + Carte.

Pour ajouter un groupe Carte + Carte:

1. Dans l'arborescence, développez l'élément **Groupes.**
2. Sélectionnez **Carte + Groupes de cartes.**
3. Dans la barre d'outils, cliquez sur l'icône 

4. Dans le champ **Description**, saisissez le nom du groupe d'entrée..
5. Cliquez sur **OK**.

La fenêtre se ferme et le nouveau groupe carte + carte apparaît dans la zone d'affichage.

9.7.2. Ajouter des utilisateurs à un groupe Carte + Carte

Une fois qu'un groupe Carte + Plan a été créé, vous devez ajouter des utilisateurs.

Pour ajouter des utilisateurs à un groupe Carte + groupe de Carte:

1. Dans l'arborescence, développez l'élément **Départements/Utilisateurs** et sélectionnez un département contenant les utilisateurs que vous souhaitez ajouter au groupe Carte + groupe de Carte..
2. Sélectionnez un utilisateur dans la zone d'affichage.
3. Dans la barre d'outils, cliquez sur l'icône 
4. In het tabblad **Algemeen** in het venster **"Gebruikerseigenschappen",** selecteert u de Kaart + Kaart groep vanuit de uitvouw lijst **"Kaart + Kaart Groep".**
5. Cliquez sur **OK**.
6. Répétez ce processus pour chaque utilisateur que vous souhaitez ajouter à un carte + groupe de carte particulier.

9.8. Groupes d'accès véhicules

Le groupe d'accès véhicule est utilisé pour définir les véhicules pour LPR.

La fonctionnalité sera traitée dans les prochaînes versions du manuel.

9.9. Ajouter un parking

L'option de gestion Parking vous permet de créer des groupes avec un nombre limité d'utilisateurs ayant accès à une certaine zone. Par exemple, un parking desservant plusieurs entreprises et chaque entreprise dispose d'un certain nombre de places de stationnement. Cette option permet de fixer une limite pour chaque entreprise et, lorsque cette limite est atteinte, aucun accès n'est plus accordé. Cette fonction est basée sur un compteur qui comptabilise le nombre d'utilisateurs dans une zone spécifique.

Cette fonction n'est pas disponible pour les panneaux de contrôle d'accès AC-215.

Il n'est possible d'ajouter qu'une seule zone de parking par panneau.

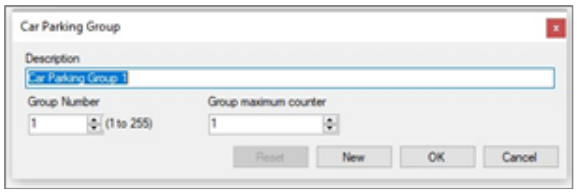
Une zone de parking ne peut être ajoutée que si une zone d'accès a été préalablement définie (voir Ajouter des zones d'accès).

Pour définir une zone de parking:

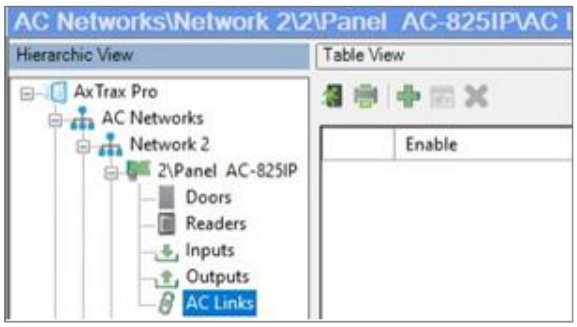
1. Créez une zone d'accès avec des lecteurs d'entrée et de sortie (voir Ajouter des zones d'accès).
2. Dans l'arborescence, cliquez sur **Car Parking**.
3. Dans la barre d'outils, cliquez sur l'icône 

4. Dans **Description**, saisissez le nom de la zone de parking.
5. Dans **Zone d'accès**, sélectionnez la zone d'accès appropriée que vous avez définie en ajoutant Zones d'accès.

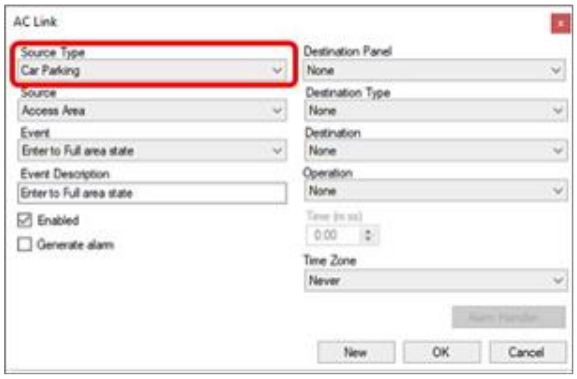
6. Dans la zone **"Vérifié par**", effectuez l'une des opérations suivantes:
   a. Sélectionnez “**Access Area”**.
      i. Dans **Area maximum counter**, sélectionnez le nombre maximal de places de parking disponibles dans cette zone d'accès.
      ii. Cliquer sur **OK**.
   b. Sélectionnez "Groupes d'utilisateurs" (**User Groups)**.
      i. Cliquer sur **OK**.
      ii. Dans l'arborescence, développez l'élément “**Car Parking”** t sélectionnez la zone de parking que vous venez de créer.
      iii. Dans la barre d'outils, cliquez sur l'icône 



      iv. Dans **Description**, entrez un nom pour le sous-groupe parking..
      v. Dans **Group maximum counter**, sélectionnez le nombre maximum de places de stationnement pour ce groupe de parking.
      vi. Cliquer sur **OK**.
      vii. Dans **l'arborescence**, développez l'élément **Departments/Users** et sélectionnez le département qui contient les utilisateurs que vous souhaitez ajouter au sous-groupe parking.
      viii. Sélectionnez un utilisateur dans la zone d'affichage.
      ix. Dans la barre d'outils, cliquez sur l'icône 
      x. Dans l'onglet **Général** de la fenêtre **Propriétés de l'utilisateur**, sélectionner le sous-groupe **Parking** dans le menu déroulant **Groupe de parking**.
      xi. Cliquez sur **OK**.
      xii. Répétez les étapes vi à xi pour chaque utilisateur que vous souhaitez ajouter à un groupe de parking.
7. Sélectionnez **AC Liens**.



8. Dans la barre d'outils, cliquez sur l'icône 
9. Dans la liste **Source Type**, sélectionnez **Car Parking**.



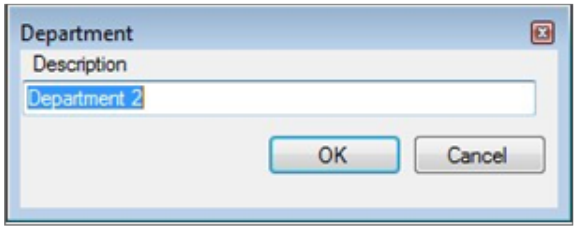
10. Gestion des utilisateurs

Chaque utilisateur est lié à un département. Pour chaque utilisateur, AxTraxPro stocke les coordonnées, les détails de la carte associée et les droits d'accès.

10.1. Ajouter des départements

Pour ajouter un département:

1. Dans l'arborescence, développez l'élément **Utilisateurs** et cliquez sur l'élément **Départements/Utilisateurs**.
2. Dans la barre d'outils, cliquez sur l'icône 



3. Dans le champ Description, saisissez le nom du département et cliquez sur **OK**.
   La fenêtre se ferme et le nouveau département apparaît dans la zone d'affichage.

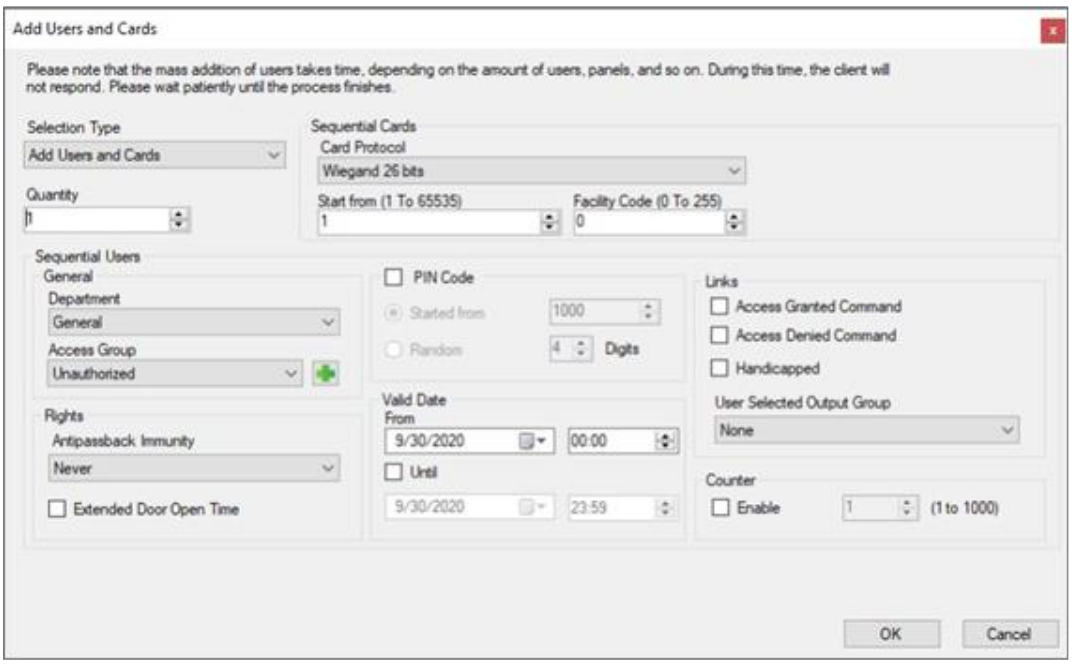
10.2. Ajouter une série d'utilisateurs et de cartes

Il est également possible d'ajouter une série d'utilisateurs et de cartes en une seule fois et de définir les éléments suivants:

- le type de lecteur nécessaire pour lire la carte
- Le nombre de cartes à créer.
- Si un utilisateur doit être créé pour chaque nouvelle carte

Pour ajouter des utilisateurs et des cartes:

1. Dans l'arborescence, sélectionnez l'élément **Utilisateurs.**
2. Dans la barre d'outils, cliquez sur l'icône 



3. Configurez les propriétés de la carte en fonction des descriptions des champs dans le tableau ci-dessous:

Champs	Description
Type de sélection	Sélectionnez ce qui sera ajouté : Utilisateurs et cartes, Utilisateurs ou cartes
Nombre	Entrez ou sélectionnez le nombre de cartes/utilisateurs à ajouter.
Cartes consécutives	Définition des propriétés de la carte: • **Type de lecteur :** choisir le type de lecteur adapté aux nouvelles cartes ajoutées. • **Start from :** Tapez le numéro de la première carte de la série. • **Code de facilité :** tapez le code de facilité pour ces cartes. Ce champ n'est pas disponible pour tous les types de lecteurs

Champs	Description
Utilisateurs séquentiels > Général	Définir les propriétés générales de l'utilisateur: • **Département :** Lier les utilisateurs nouvellement créés à un département. • **Groupe d'accès :** Lier l'utilisateur nouvellement créé à un groupe d'accès. Cliquer sur  pour ajouter l'utilisateur à un groupe d'accès personnalisé parmi tous les lecteurs disponibles.
Utilisateurs séquentiels> Droits	Définir les propriétés des droits des utilisateurs: • **Antipassback Immunity (Immunité anti-passback) :** Choisir comment passer outre les restrictions anti-passback : Jamais, Toujours, selon le fuseau horaire. • **Temps d'ouverture de la porte prolongé :** Sélectionner pour activer l'option de porte prolongée définie pour chaque porte.
Utilisateurs séquentiels > Code PIN	Pour définir des codes PIN automatiques, sélectionnez entre: • **Commencer à partir de :** Code PIN séquentiel à partir d'un numéro prédéfini basé sur un nombre défini de chiffres. • **Aléatoire :** codes PIN aléatoires où la seule définition est le nombre de chiffres du code PIN.
Utilisateurs séquentiels > date de validité	Déterminer la validité du droit d'accès: • **Du : Définissez la date et l'heure auxquelles l'accès doit commencer à être accordé.**. • **Jusqu'au :** Sélectionnez cette option pour définir une date de fin de validité du droit d'accès, puis définissez la date et l'heure.
Utilisateurs séquentiels > Liens	Sélectionnez cette option pour définir les AC liens associés: • **Case à cocher Accès accordé :** Active un ensemble d'entrées ou de sorties défini par l'utilisateur pour les événements pour lesquels l'accès est autorisé. • **Case à cocher Accès refusé :** Active un ensemble d'entrées ou de sorties définies par l'utilisateur pour les événements où l'accès est refusé. • **Case à cocher Handicapés :** active une sortie spéciale peu après le déverrouillage de la porte. Les sorties sont définies dans la fenêtre AC Liens. • **User selected Output group (Groupe de sorties sélectionné par l'utilisateur) :** sélectionnez un groupe de sorties pour cet utilisateur. Les sorties sont activées chaque fois que l'utilisateur franchit une porte. Les opérations, les entrées et les sorties sont définies dans la fenêtre AC Liens (voir **Ajouter des liens entre les panneaux**).
Utilisateurs séquentiels > Compteurs	Sélectionnez Activer pour utiliser l'option compteur, puis tapez ou sélectionnez le numéro du compteur à utiliser pour le premier utilisateur.

4. Cliquez sur **OK** pour fermer la fenêtre.

Le processus peut durer plusieurs minutes, après quoi une boîte de dialogue signale que l'opération est terminée.

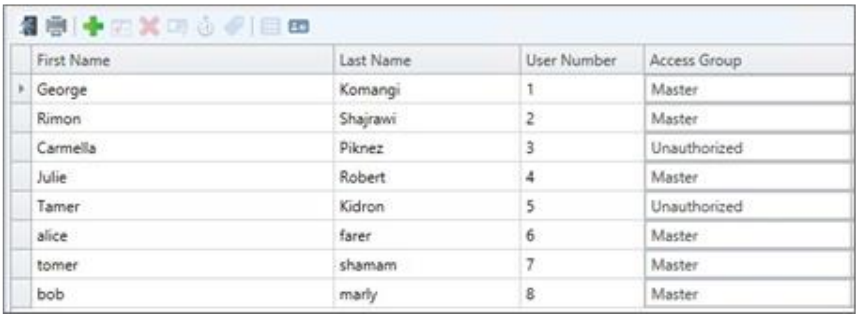
10.3. Affichage des utilisateurs

Les utilisateurs peuvent être affichés dans une liste ou sous la forme d'un groupe de cartes.

Pour afficher les utilisateurs dans une liste:

1. Dans l'arborescence, sélectionnez le département des utilisateurs à afficher.

2. Cliquez sur l'icône Liste.

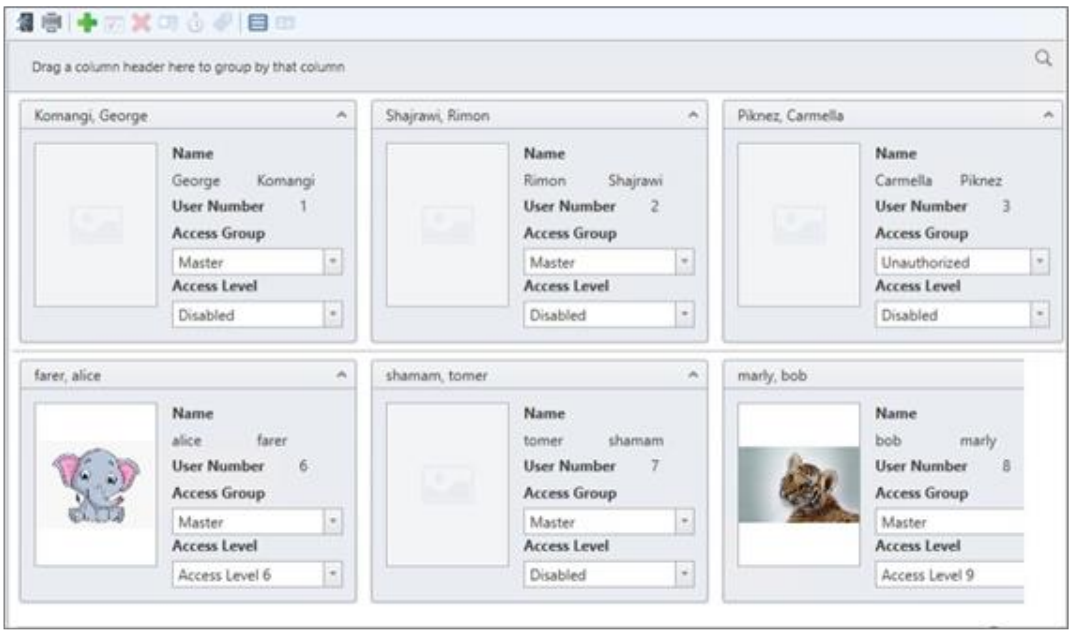


First Name	Last Name	User Number	Access Group
George	Komangi	1	Master
Rimon	Shajrawi	2	Master
Carmella	Piknez	3	Unauthorized
Julie	Robert	4	Master
Tamer	Kidron	5	Unauthorized
alice	farer	6	Master
tomer	shamam	7	Master
bob	marly	8	Master

Pour afficher les utilisateurs sous forme de groupe de cartes:

1. Dans l'arborescence, sélectionnez le département des utilisateurs à afficher.

2. Cliquez sur l'icône Carte.



10.4. Ajouter un utilisateur individuel

Pour ajouter un utilisateur individuel :

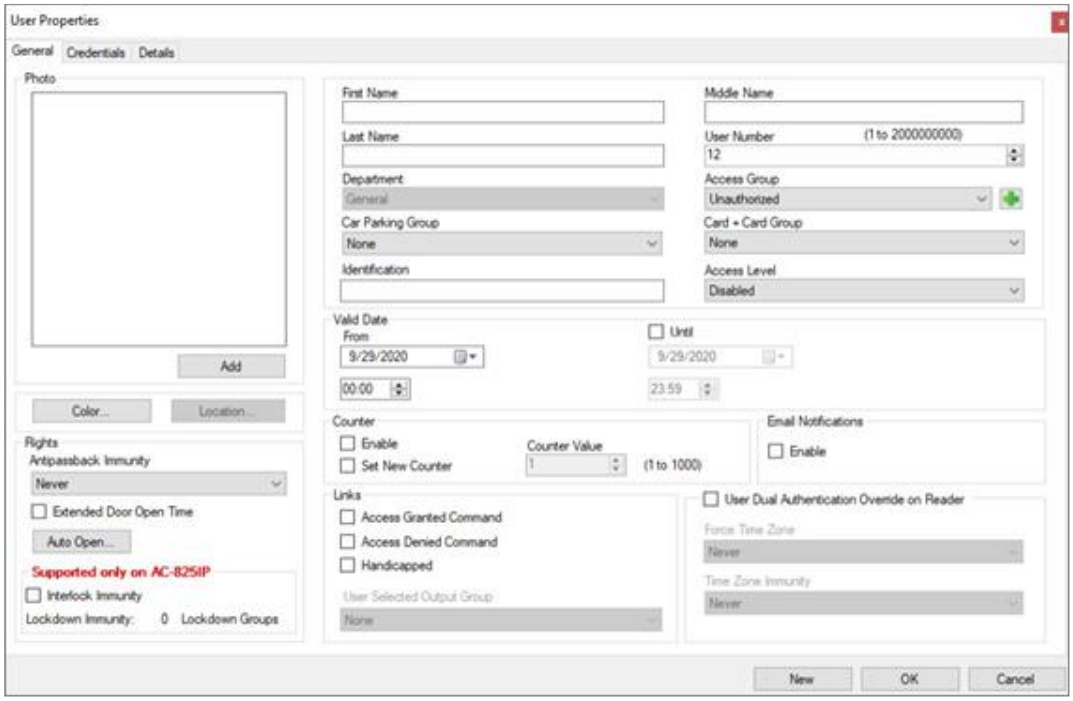
1. Dans l'arborescence, développez l'élément **Utilisateurs**.
2. Développez l'élément **Départements/Utilisateurs** et sélectionnez un département pour le nouvel utilisateur.
3. Dans la barre d'outils, cliquez sur l'icône 
4. Entrez les données utilisateur requises à l'aide des onglets décrits dans les sous-sections ci-dessous.
5. Cliquer sur **OK**.

   La fenêtre se ferme et le nouvel utilisateur apparaît dans la zone d'affichage.

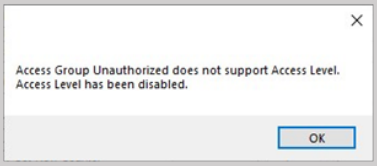
10.4.1. Général

L'onglet **Général** affiche:

- Les informations d'identification de l'utilisateur
- Les paramètres de validité de l'utilisateur
- Les droits d'accès de l'utilisateur



L'onglet Général est décrit dans le tableau suivant:

Champs	Description
Photo > Ajouter	Cliquez pour ajouter une photo d'utilisateur ou supprimer une photo existante. Le ratio de la photo sélectionnée doit être de 1,25 H x 1,00 L, sinon la photo risque d'être déformée. Assurez-vous que la photo est correctement tournée avant de l'ajouter.
Prénom	Entrez ici le prénom de l'utilisateur
Deuxième prénom	Entrez ici le deuxième prénom de l'utilisateur
Nom de famille	Entrez le nom de l'utilisateur ici
Numéro d'utilisateur	Entrez un numéro d'utilisateur unique pour identifier l'utilisateur.
Département	Sélectionner le département de l'utilisateur concerné
Groupe d'accès	Sélectionnez le groupe d'accès de l'utilisateur Par défaut, ce groupe est défini comme Refusé Cliquer sur  pour ajouter des utilisateurs à un groupe d'accès personnalisé parmi tous les lecteurs disponibles et les terminaux mappés.
Groupe parking véhicules	Sélectionnez cette option pour ajouter un utilisateur à un groupe de parking de véhicules défini.
Groupe carte + carte	Sélectionnez cette option pour ajouter un utilisateur à un groupe Carte + Carte.
Identification Niveau d'accès	Ajouter du texte pour identifier l'utilisateur Sélectionner le niveau d'accès Aucun niveau d'accès ne peut être sélectionné pour un utilisateur dans un groupe d'accès "Refusé". 
Couleur	Cliquez pour sélectionner la couleur à utiliser pour marquer cet utilisateur lorsqu'il génère des événements d'accès. Le marquage de l'utilisateur doit être activé dans **Outils > Options > onglet Général.**
Location	Cliquez pour afficher un journal des portes ouvertes par cet utilisateur.
Date de validité > A partir de Date de validité > Jusqu'au	Sélectionnez la date/heure à laquelle les droits d'accès de l'utilisateur commencent. Sélectionnez la date/heure à laquelle les droits d'accès de l'utilisateur prennent fin. Ce champ n'est disponible que si la case à cocher est sélectionnée. Pour les panneaux AC-215, seule la date est reconnue ; l'heure saisie n'est pas reconnue. De plus, la date " jusqu'au " ne fait pas partie de la zone valide.
Compteur > Activer	Sélectionnez cette option pour définir un compteur de droits d'accès pour cet utilisateur (voir **Configuration des compteurs d'utilisateurs**). Lorsque le compteur atteint zéro, l'utilisateur n'a plus d'accès.
Compteur > Définir un nouveau compteur	Sélectionnez cette option pour définir une nouvelle valeur de compteur de compte à rebours pour cet utilisateur (voir **Configurer les compteurs d'utilisateurs**).
Compteur > Valeur du compteur	Sélectionnez cette option pour définir une nouvelle valeur de compteur pour cet utilisateur. Ce champ n'est activé que si la case **Définir un nouveau compteur** est cochée..
Notifications par e-mail > Activer	Cochez cette case pour envoyer des notifications par courriel à l'adresse électronique de l'utilisateur définie dans l'onglet Détails (voir **l'onglet Détails)**
Droits > Immunité anti-passback	Cochez cette case pour supprimer toutes les restrictions Antipassback pour cet utilisateur. • **Jamais** • **Toujours** • **Fuseau horaire défini par l'utilisateur** Pour un panneau AC-215, seul Always fonctionne.

Droits > Temps d'ouverture prolongé de la porte	Sélectionnez cette option pour permettre à cet utilisateur de bénéficier d'une durée d'ouverture de porte prolongée. La durée prolongée est définie pour chaque porte (voir **AC-825IP**)
Droits > Ouverture automatique	Lors de la définition des propriétés de l'utilisateur, il est possible de spécifier que certains groupes de sortie sont automatiquement actifs (voir **Ouverture automatique des groupes de sortie**).
Autorisations > Immunité d'Interlock	Cela permet à l'utilisateur d'ouvrir les portes du groupe d'accès concerné, quel que soit l'état de la serrure. Cette fonction ne fonctionne que pour l'AC-825IP
Liens > Commande Accès autorisé	Sélectionnez cette option pour activer un AC Lien initiée par les commandes auxquelles cet utilisateur a accès (voir **Ajouter des liens entre les panneaux**).
Liens > Commande Accès refusé	Sélectionnez cette option pour activer un AC Lien initiée par des commandes d'accès refusées pour cet utilisateur (voir **Ajouter des liens au panneau**).
Liens > Handicapés	Sélectionnez cette option pour activer une sortie spécifique peu après le déverrouillage de la porte (voir **Ajouter des liens de panneau**).
Liens > Groupe de sortie sélectionné par l'utilisateur	Sélectionnez un groupe de sorties pour cet utilisateur. Les sorties sont activées chaque fois que l'utilisateur entre dans une porte, comme spécifié dans la fenêtre Lien (voir **Ajouter des liens dans le panneau**).
Authentification double utilisateur Activation du lecteur	Sélectionnez cette option pour annuler la double authentification définie par le système. • **Force Time Zone**: l'utilisateur doit présenter deux justificatifs d'identité même si le lecteur ne l'exige pas. Pour activer cette fonction, la case Mode double authentification doit être cochée dans la fenêtre du lecteur. • **Time Zone Immunity**: L'utilisateur se voit accorder l'accès pour un seul badge et non pour deux badges différents, même si le lecteur est en mode "double authentification de l'utilisateur".

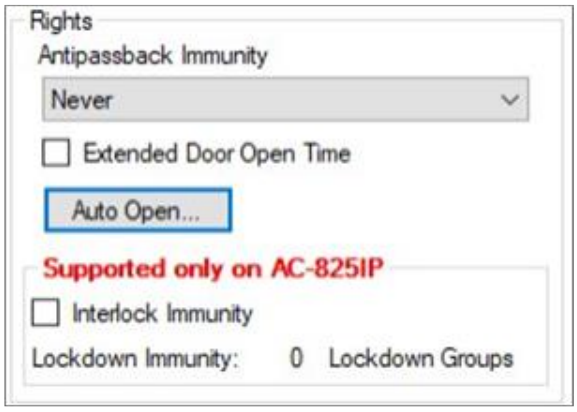
10.4.1.1. Ouverture automatique des groupes de sortie

Lors de la définition des propriétés de l'utilisateur, vous pouvez configurer certains groupes de sorties pour qu'ils deviennent automatiquement actifs.

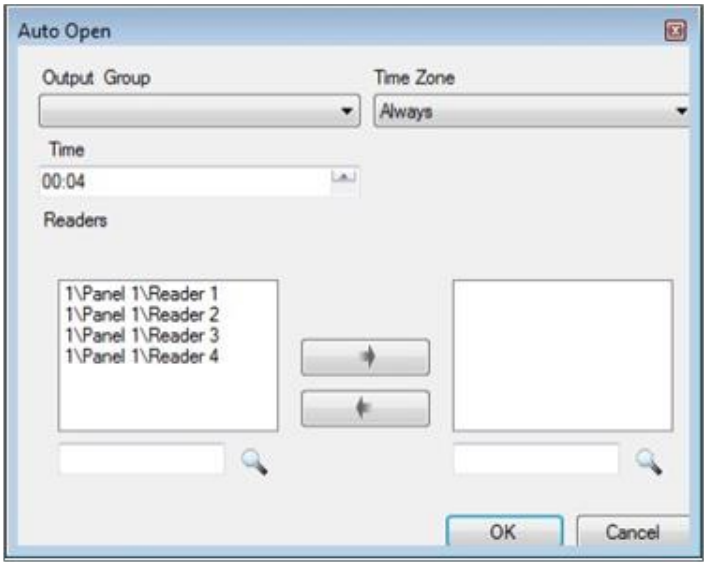
Pour activer cette fonction, les sorties doivent toujours être actives dans le "Filtre d'événements" (Propriétés du panneau > Option).

Pour définir l'ouverture automatique des groupes de sorties:

1. Dans la section “Rights”, cliquer sur “**Auto open”**.



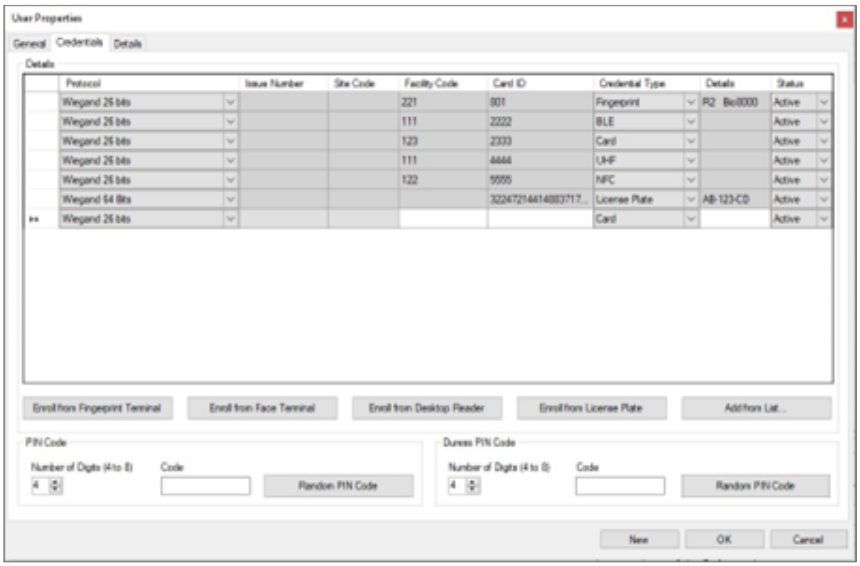
2. Pour chaque groupe de sortie sélectionné (**Output Group**) dans le menu déroulant Groupe de sortie:
   a. Sélectionnez un fuseau horaire dans le menu déroulant Fuseau horaire (**Timezone)**.
   b. Dans la case Temps (**Time**), sélectionnez une durée d'activation.
   c. Sélectionnez et déplacez les lecteurs souhaités à l'aide des flèches.



3. Cliquer sur **OK**.

10.4.2. Onglet Identifiants (Credentials)

L'onglet "**Credentials**" permet d'associer jusqu'à 16 cartes à chaque utilisateur et d'attribuer un code PIN à l'utilisateur.



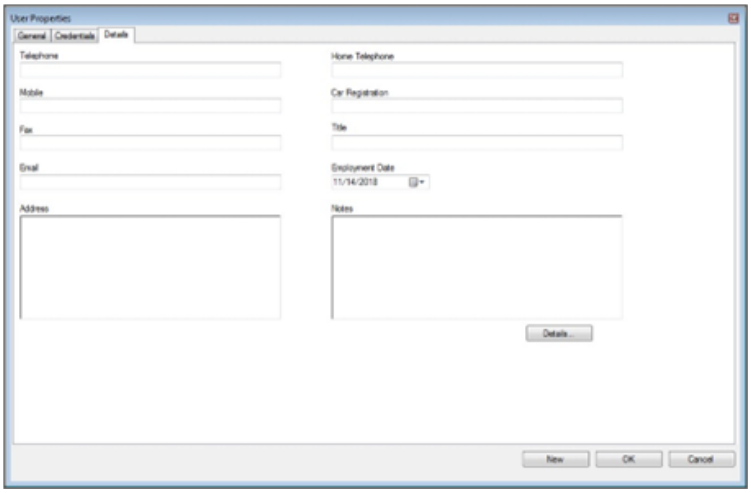
Champs	Description
Détails	Affiche les différentes propriétés de l'identifiant ajouté au système pour l'utilisateur. Les champs Numéro de délivrance et Code de localisation ne sont disponibles que si le protocole sélectionné est "Rosslare 38-Bit (Rosslare property)
Détails > Enregistrement à partir de l'empreinte digitale	Cliquez sur le bouton pour enregistrer l'empreinte digitale d'un utilisateur (voir **Enregistrement de l'empreinte digitale d'un utilisateur)**
Détails> enregistrer à partir du plaque d'immatriculation	Cliquez sur le bouton pour enregistrer une plaque d'immatriculation (voir **Enregistrement d'une plaque d'immatriculation**).
Détails>Enregistrement à partir du terminal facial terminal	Cliquez sur le bouton pour enregistrer un visage à partir d'un terminal (voir **Enregistrer un visage à partir d'un terminal).**
Détails>Enregistrement à partir du lecteur de bureau	Cliquez sur pour enregistrer les données avec un lecteur de bureau

Détails > Ajouter à la liste	Cliquez sur le bouton pour associer un utilisateur à une carte ou à plusieurs cartes (voir **Associer un utilisateur à une carte**). Avant de lier un utilisateur à une carte, assurez-vous que la carte a été ajoutée au système (voir **Ouverture automatique des groupes de sortie**) Toutes les cartes du code d'installation spécifié par l'utilisateur sont énumérées.
PIN code / Duress PIN code	• Options de définition du code PIN et du code PIN sous contrainte • Nombre de chiffres : Sélectionnez la longueur du code PIN pour cet utilisateur. • Code : Le code PIN de 4 à 8 chiffres et/ou le code PIN de contrainte • Code PIN aléatoire : cliquez sur ce bouton pour générer automatiquement un code PIN aléatoire.

	AxTraxPro permet de définir tous les chiffres, y compris les zéros, pour le code PIN/Code PIN de détresse.

10.4.3. Onglet Détails

L'onglet **Détails** contient des informations détaillées sur le contact et l'identification de cet utilisateur..



Les champs de l'onglet Détails sont décrits dans le tableau suivant :

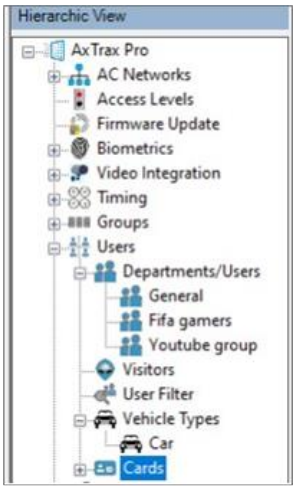
Champs	Description
Téléphone	Insérer le numéro de téléphone professionnel de l'utilisateur.
Mobile	Insérer le numéro de téléphone portable de l'utilisateur.
Fax	Insérer le numéro de fax de l'utilisateur.
Email	Insérer l'adresse e-mail de l'utilisateur (100 caractères maximum).
Adresse du domicile	Insérer l'adresse postale de l'utilisateur
Téléphone privé	Insérer le numéro de téléphone du domicile de l'utilisateur.
Plaque d'immatriculation du véhicule	Insérer le numéro d'immatriculation du véhicule de l'utilisateur.
Titre	Insérer le titre de l'utilisateur (par exemple "M.").
Date de début d'emploi	Inscrire la date à laquelle l'utilisateur a commencé à travailler.
Remarques	Insérer toute information complémentaire.
Détails	Cliquez sur pour ouvrir le dossier d'informations complémentaires de l'utilisateur.

10.5. Gestion des cartes

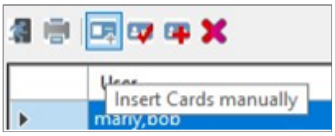
Les cartes d'accès sont ajoutées manuellement au système. L'enregistrement d'une carte se fait via un lecteur de bureau ou un lecteur UHF. Une fois qu'une carte est ajoutée au système, elle peut être associée à un utilisateur.

Pour ajouter des cartes manuellement

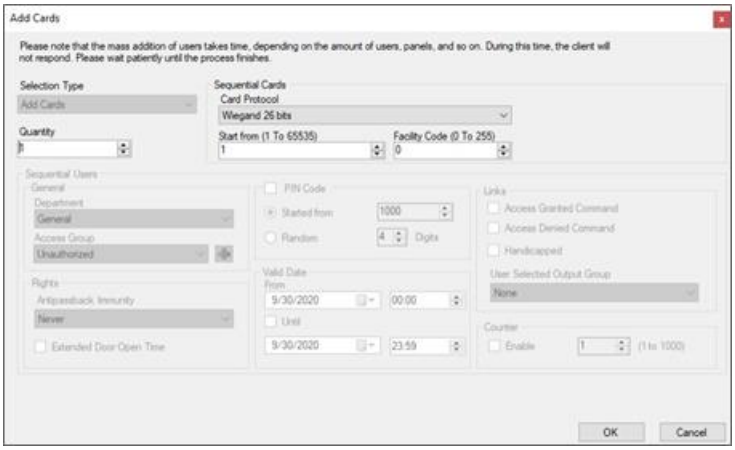
1. Dans l'arborescence **Utilisateurs**, sélectionnez **Cartes**



2 Cliquez sur l'icône **Insert Cards manually**



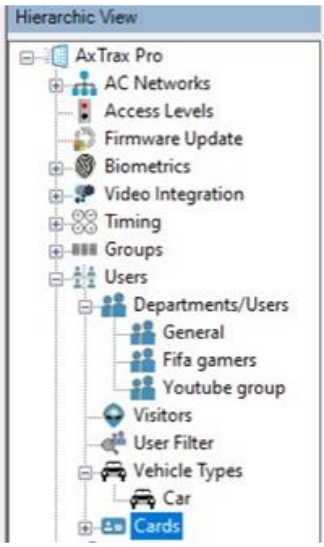
3. Tapez ou sélectionnez la quantité, le numéro de la première carte et le code de facilité dans la case appropriée.



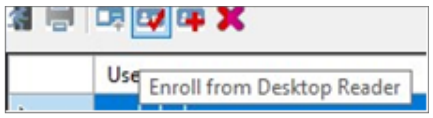
4. Cliquer sur **OK**.

Pour programmer les cartes à l'aide d'un lecteur de bureau:

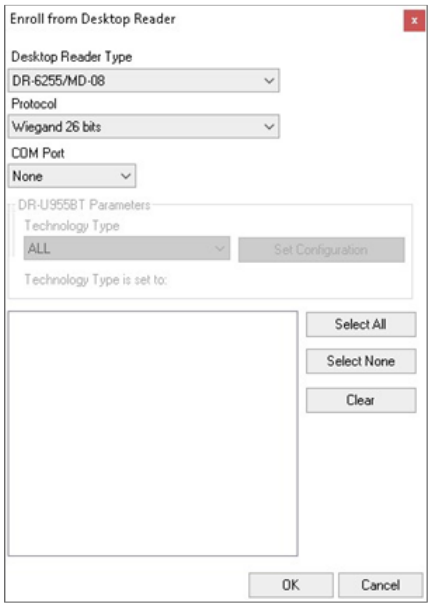
1. Dans l'arborescence **Utilisateurs**, sélectionnez **Cartes**.



2. Cliquez sur l'icône  **Enroll from Desktop Reader**

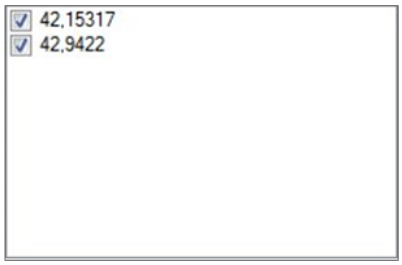


3. Sélectionnez le type **Desktop Reader**, **Protocol**, et **COM Port** dans la liste correspondante.



4. Si le DR-U955BT est sélectionné sous **Type de lecteur de bureau**, vous devez également sélectionner le type de technologie dans le menu déroulant et cliquer sur **Définir la configuration**.

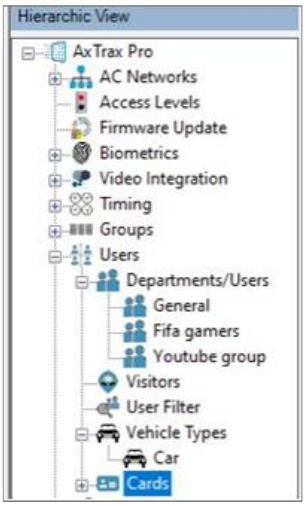
5. Programmer une carte en la présentant au lecteur. Chaque carte programmée apparaît à l'écran.



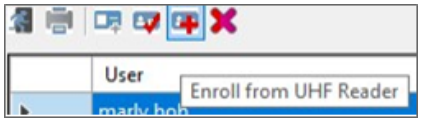
6. Sélectionner les cartes à ajouter (les cartes ajoutées sont sélectionnées par défaut).
7. Cliquer sur **OK**.

Pour enregistrer des cartes à partir d'un lecteur UHF:

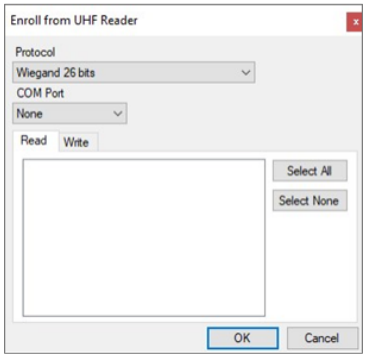
1. Dans l'arborescence **Utilisateurs**, sélectionnez **Cartes**.



3 Cliquez sur l'icône  **Enroll from UHF Reader**



3. Sélectionnez le **protocole** et le **port COM** dans la liste correspondante.



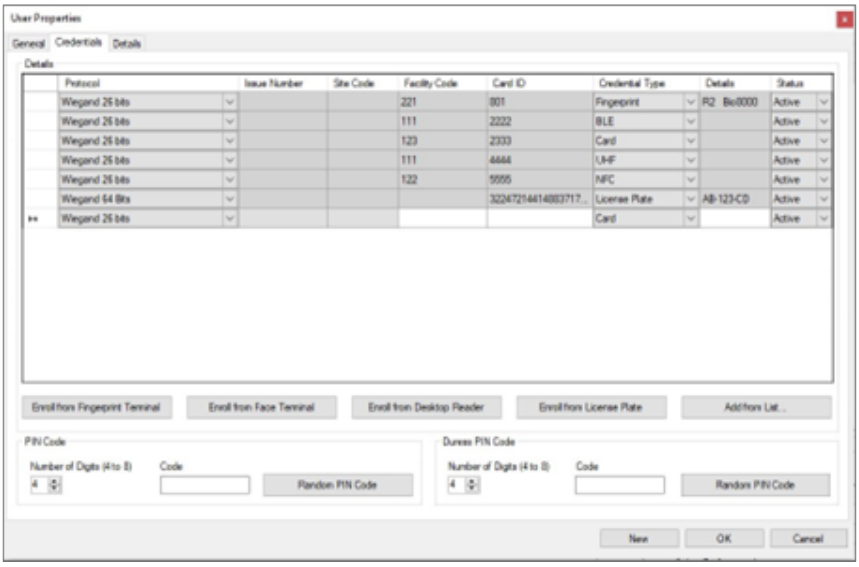
4. Cliquer sur **OK**.

10.5.1. Associer un utilisateur à une carte

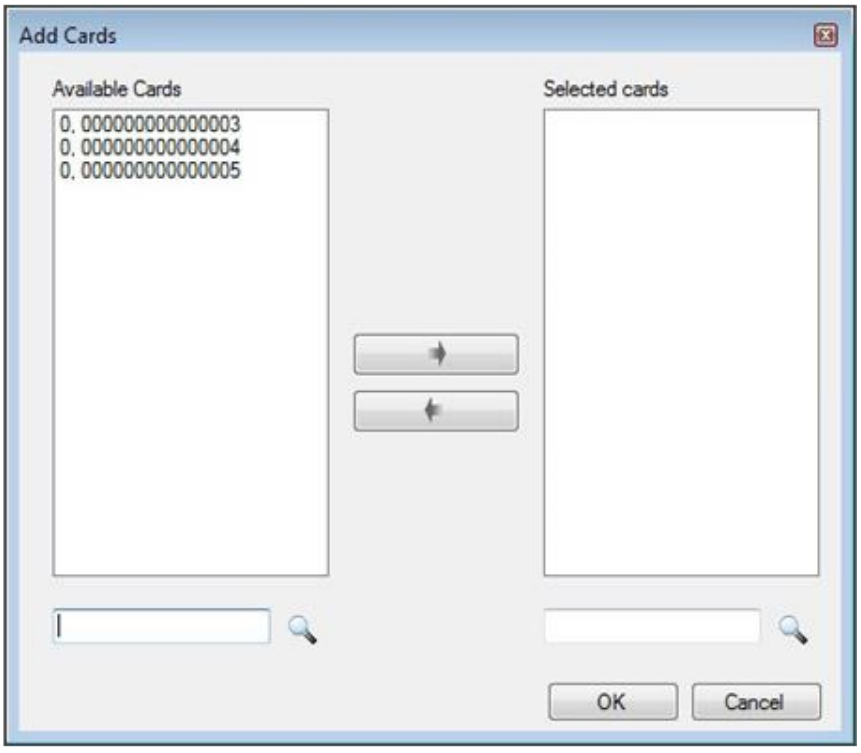
Après avoir ajouté des utilisateurs et des cartes au système, vous devez associer chaque utilisateur à une carte.

Pour associer un utilisateur à une carte:

1. Dans la fenêtre Propriétés de l'utilisateur **(User Properties)**, cliquez sur l'onglet Identifiants (**Credentials)**.



4 Cliquer sur **Add from List**.



3. Dans la liste des cartes disponibles, sélectionnez la ou les cartes que vous souhaitez associer à l'utilisateur et déplacez-les vers le panneau de droite à l'aide des flèches.

> Als Si une carte est déjà associée à cet utilisateur, elle apparaîtra dans la liste des cartes sélectionnées (**Selected Cards).**

4. Cliquez sur **OK.**

   Vous pouvez également ouvrir la fenêtre **Ajouter des cartes** via l'arborescence..

5. Dans l'arborescence, développez l'élément **Utilisateurs** et développez l'élément **Départements/Utilisateurs**.
6. Sélectionnez un département qui contient les utilisateurs que vous souhaitez associer à une carte et sélectionnez un utilisateur dans le tableau.

7. Cliquez sur l'icône 

10.5.2. Création de cartes (PhotoID)

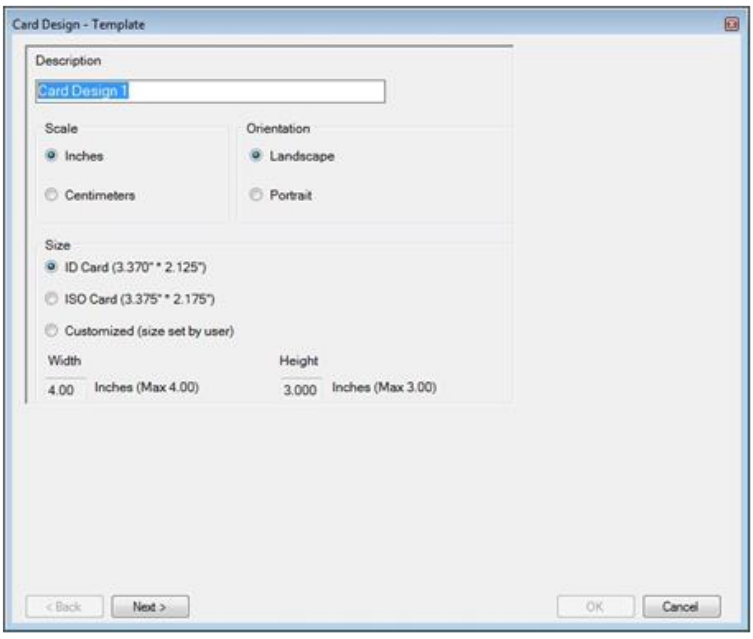
AxTraxPro permet de créer des badges pour l'impression en masse et supporte la connectivité avec des caméras numériques pour la capture d'images.

10.5.2.1. Création d'un modèle de carte

Pour créer un modèle de carte:

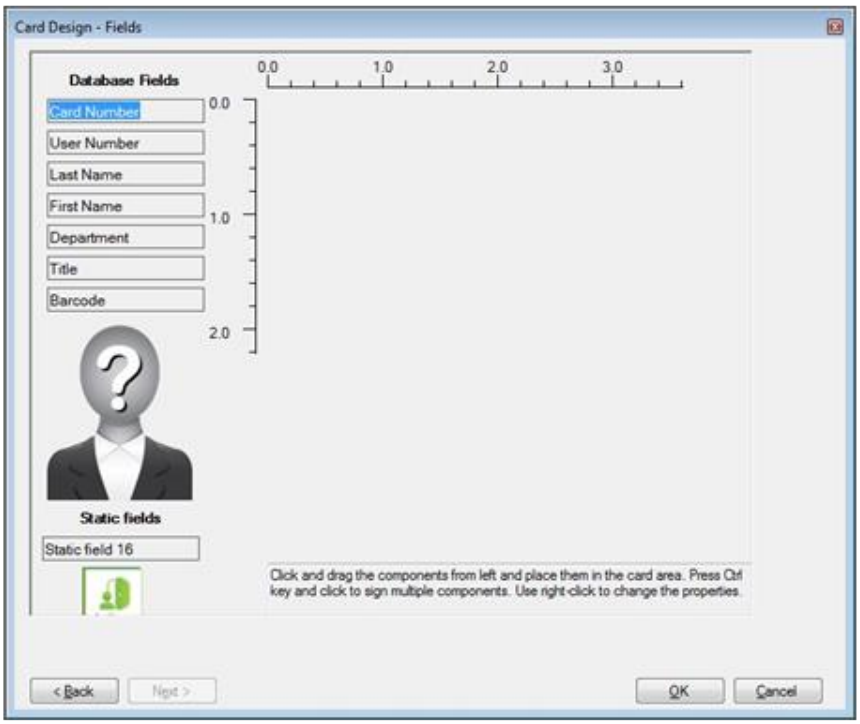
1. Dans **l'arborescence**, développez l'élément **Utilisateurs**.
2. Développez l'élément **Cartes**, puis cliquez sur Création de cartes (**Card Design)**.

3. Dans la barre d'outils, cliquez sur l'icône 

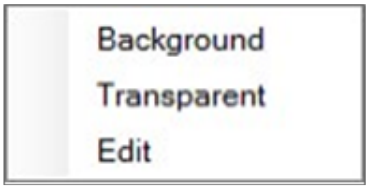


4. Entrez une description pour le modèle et définissez son échelle, son orientation et sa taille.

5. Cliquer sur **Next**

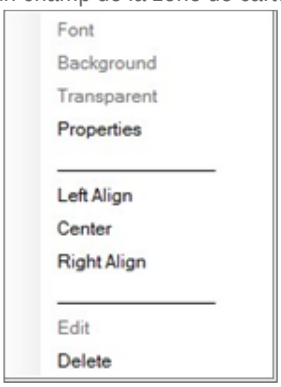


6. liquez avec le bouton droit de la souris sur l'arrière-plan de la zone de carte pour définir la couleur de l'arrière-plan ou sélectionnez un fichier à utiliser comme arrière-plan.

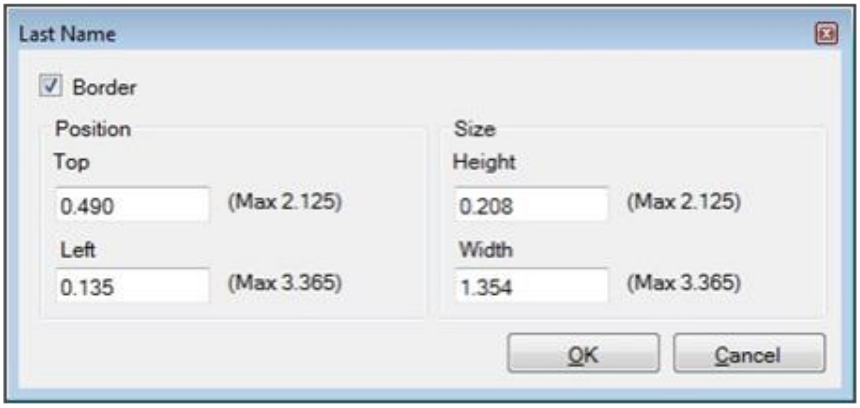


7. Faites glisser les champs situés à gauche de la zone de carte pour créer la présentation de la carte.

Cliquez avec le bouton droit de la souris sur un champ de la zone de carte pour afficher les options de menu suivantes



8. Cliquez sur Propriétés pour supprimer la marge et modifier la taille du champ.



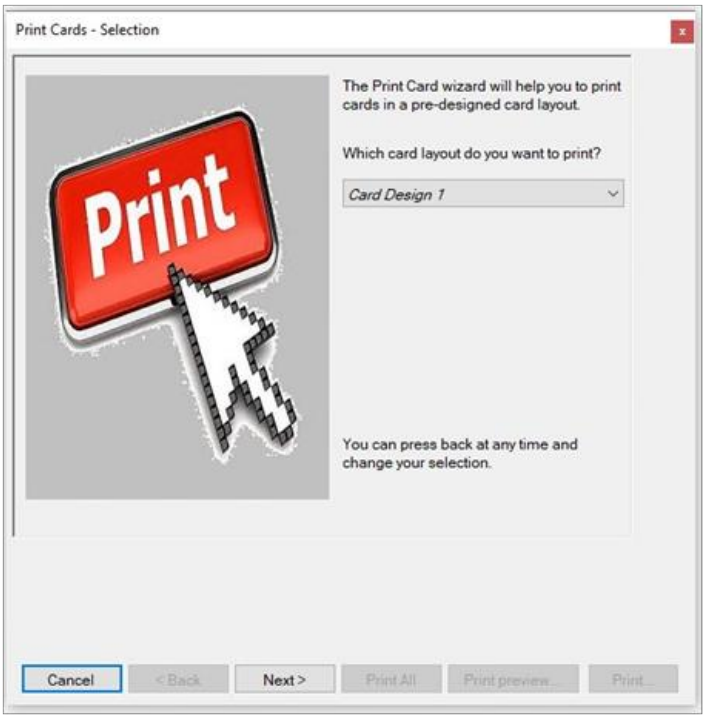
9. Cliquez sur **OK** pour revenir à l'écran Création de carte – Champs (**Card Design – Fields)**.
10. Cliquez sur **OK** pour enregistrer le modèle de carte.

10.5.2.2 Imprimer une carte

Une fois que vous avez enregistré un modèle de carte, vous pouvez imprimer des cartes à l'aide de ce modèle.
Pour obtenir les meilleurs résultats d'impression, il est fortement recommandé d'utiliser 300 dpi (dot par inch) et une résolution d'écran élevée (au moins 1280x1024 pour une carte en format portrait ou 1600x900 pour une carte en format paysage). Une résolution de 1920x1080 est recommandée.

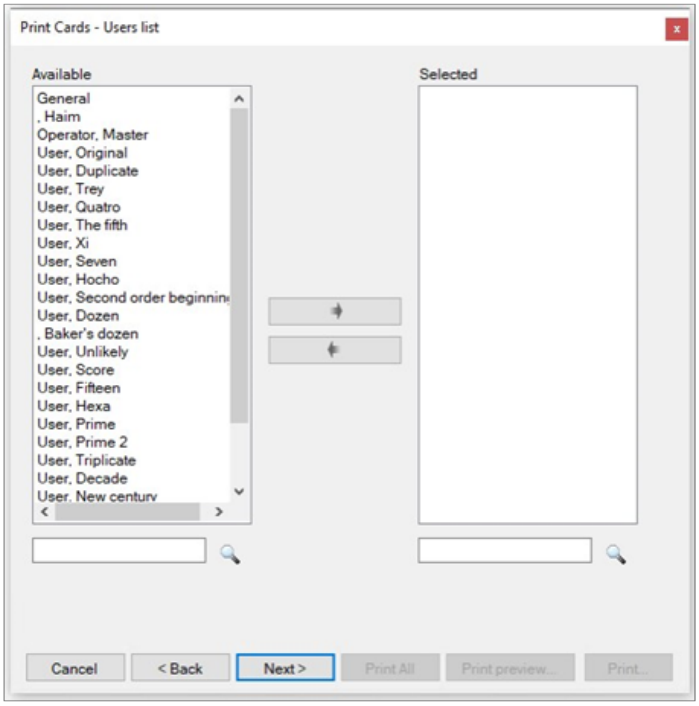
Pour imprimer une carte:

1. Dans la liste des modèles de carte de la zone d'affichage, sélectionnez le modèle que vous souhaitez utiliser et cliquez sur l'icône. 



2. Sélectionnez la mise en page que vous souhaitez utiliser (si elle est différente de celle que vous avez sélectionnée à l'étape 2 Dans la liste des modèles de carte de la zone Affichage, sélectionnez le modèle que vous souhaitez utiliser et cliquez sur l'icône), dans les listes déroulantes correspondantes.
3. Cliquer sur **Next**.

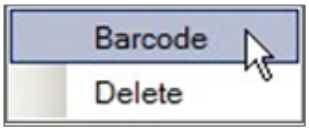
Les utilisateurs ne peuvent apparaître dans la liste des utilisateurs disponibles que si des cartes leur sont associées, comme décrit dans la section Associer un utilisateur à une carte.



4. Sélectionnez dans la liste disponible les utilisateurs pour lesquels vous souhaitez imprimer une carte et déplacez-les vers le panneau de droite à l'aide des flèches.
5. Cliquer sur **Next**

6. Changer le type de Code à bare.

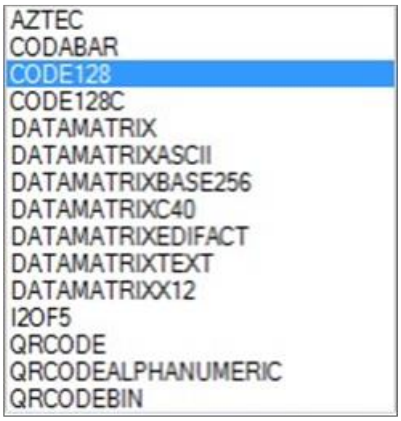
   a. Changer le type de code-barres
   cliquez avec le bouton droit de la souris sur le champ Code à barres et sélectionnez **Code à barres.**



Vous pouvez utiliser le code à barres généré automatiquement ou saisir manuellement un code à barres numérique.

Si vous sélectionnez **Numéro d'utilisateur**, le code à barres sera le même que le numéro d'utilisateur.

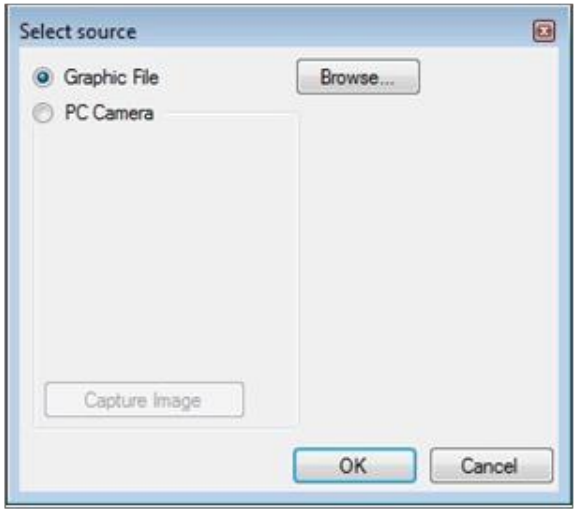
b. Dans le menu déroulant Choisir le codage alphabétique, (**Choose Alphabet coding)**, sélectionnez le type de codage



c. Cliquez sur **OK.**

Le code à barres apparaît sur le modèle de carte.

7. Cliquez sur Ajouter une photo (**Add photo)** i vous souhaitez sélectionner une autre image à partir d'un fichier ou d'un appareil photo PC:



a. Effectuez l'une des étapes suivantes:

- Sélectionnez **Parcourir** pour trouver l'image que vous souhaitez insérer.
- Sélectionnez **Caméra PC** et sélectionnez **Capturer l'image**.

a. Cliquez sur **OK.**

8. Utilisez les flèches vertes pour afficher les utilisateurs supplémentaires.
9. [Optionnel] Cliquez sur **Aperçu avant impression** pour afficher l'écran de la carte agrandie.

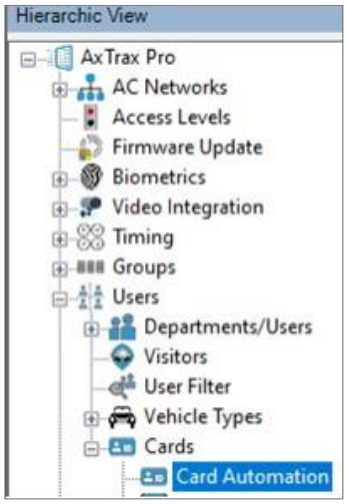
10. Cliquez sur **Imprimer** pour imprimer cette carte spécifique ou cliquez sur Imprimer tout pour imprimer toutes les cartes disponibles.

10.5.3. Configuration de l'automatisation des carte

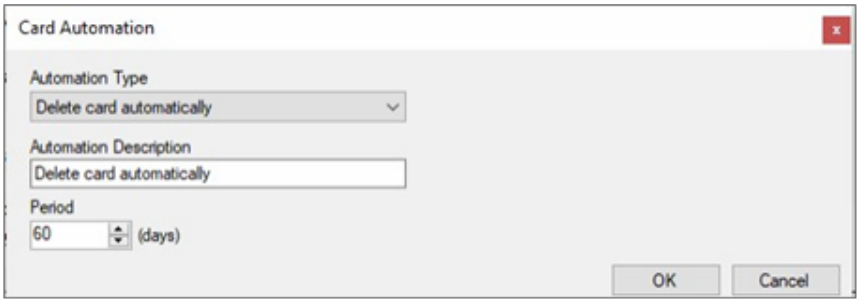
Vous pouvez programmer le système pour qu'il garde automatiquement la trace d'une carte d'utilisateur qui a expiré parce qu'elle n'a pas été utilisée pendant une certaine période. Une fois cette carte détectée, elle peut être automatiquement retirée ou vous pouvez en être averti.

Pour configurer l'automatisation des cartes:

1. Dans l'arborescence **Utilisateurs**, développez l'élément **Cartes** et sélectionnez **Automatisation des cartes**.



2. Cliquez sur l'icône 



3. Dans le menu déroulant **Type Automatisation**, sélectionnez l'action à effectuer lorsqu'une carte n'a plus été utilisée pendant une certaine période.
   - Supprimer la carte automatiquement
   - Demander avant de supprimer la carte
   - Notification par e-mail
   - Rapport dans le journal des événements du système uniquement

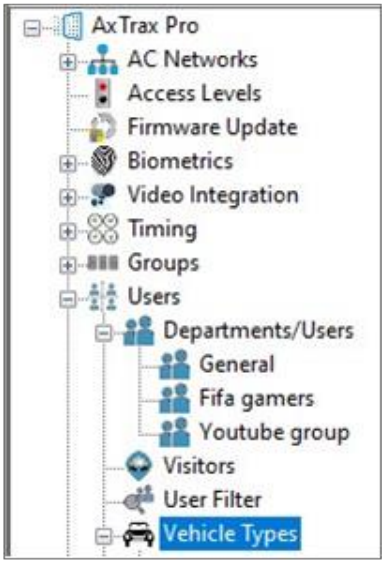
   Cette option requiert une adresse e-mail et vous pouvez ajouter une signature facultative.

4. Dans la section **Période**, sélectionnez Période de temps
5. Cliquer sur **OK**.

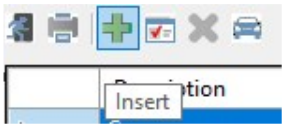
10.6. Ajouter des types de véhicules

Pour ajouter une voiture et sélectionner un type de véhicule:

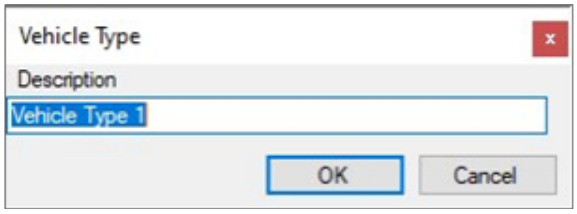
1. Dans l'arborescence, sélectionnez **Types de véhicules.**



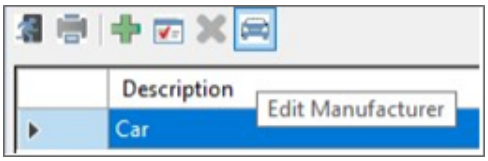
2. Cliquer sur **l'icône Insert**



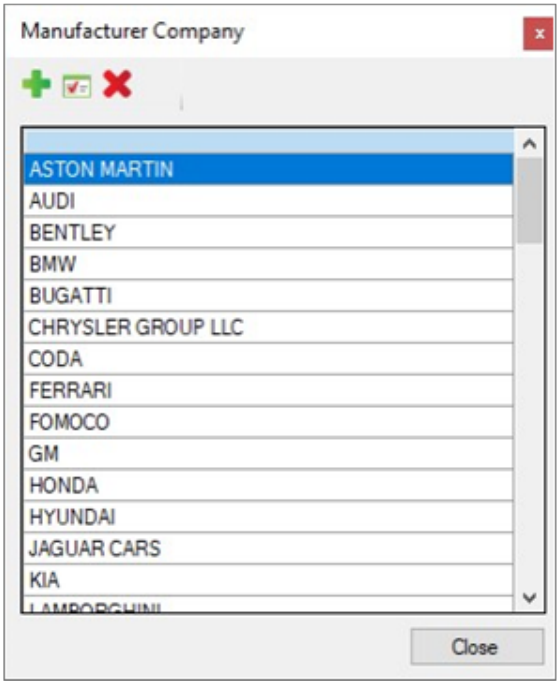
3. Entrez une **Description** pour le type de véhicule**.**



4. Cliquez sur l'icône **Edit Manufacturer**



5. Sélectionner le constructeur du véhicule dans la liste



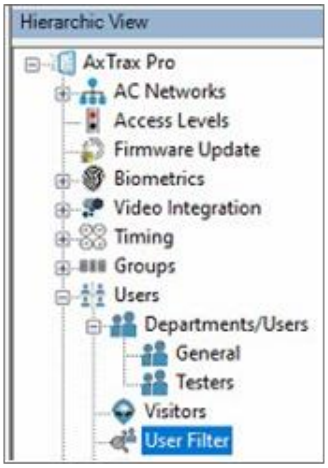
5. Cliquer sur **Close**.

10.7. Utiliser le filtre utilisateur pour rechercher des utilisateurs

Le filtre utilisateur (**User Filter)**.permet de rechercher des personnes enregistrées dans le système de contrôle d'accès

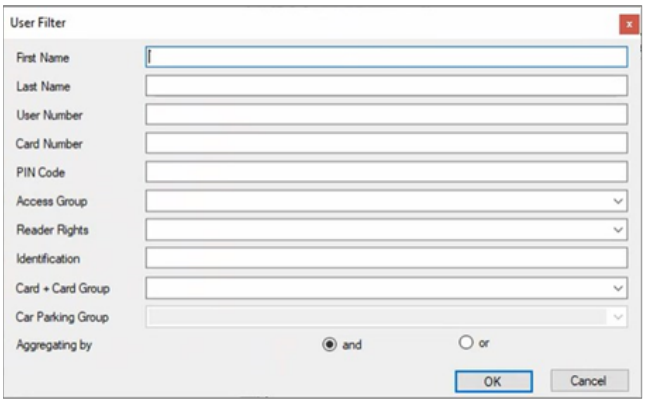
Pour rechercher des utilisateurs:

1. Dans l'arborescence, développez l'élément **Utilisateurs.**
2. Sélectionnez **User Filter**.



3. Cliquer sur 

4. Entrez les informations nécessaires à l'utilisateur



5. Cliquer sur **OK**.

Le filtre de recherche n'est pas sensible à la casse.

11. Ajouter des opérateurs

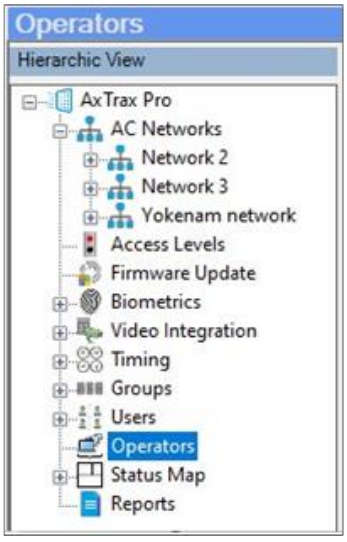
Les opérateurs sont des personnes ayant accès à l'application AxTraxPro. Le nom de l'opérateur par défaut est Administrateur.

Différents opérateurs ont des droits de sécurité plus étendus ou plus limités, allant du contrôle total du système à la possibilité de ne visualiser qu'une seule section. Tous les mots de passe des opérateurs sont sensibles à la casse.

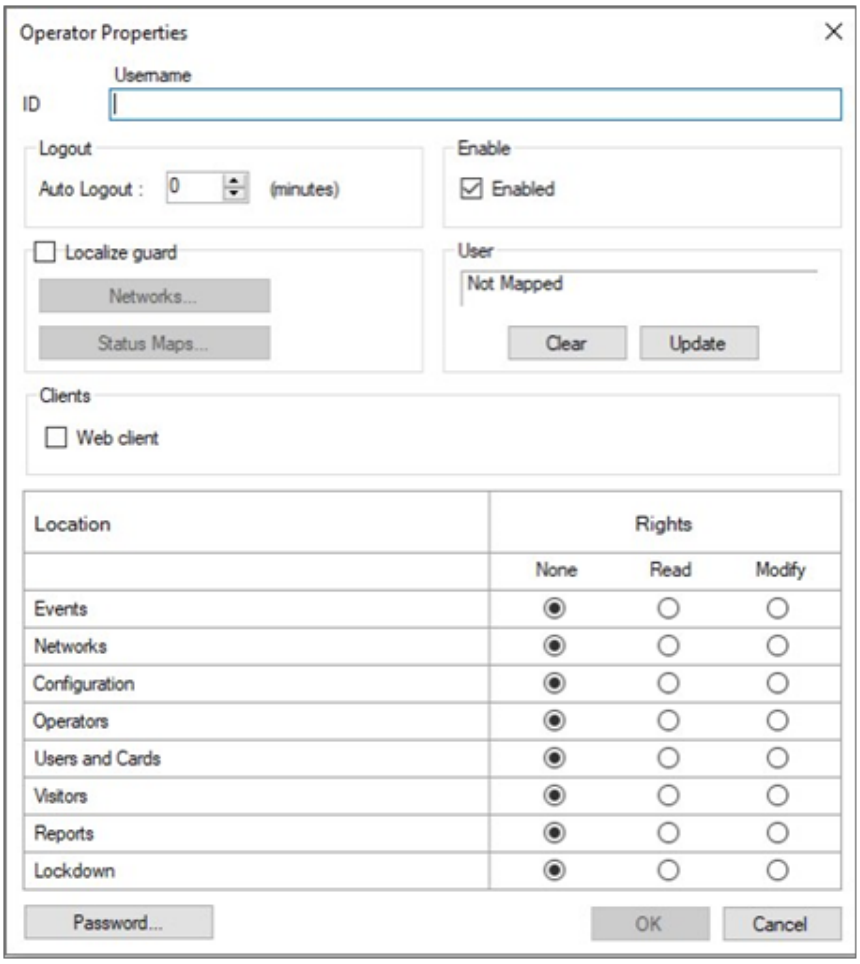
Une personne ne peut être classée dans la catégorie des opérateurs que si elle est un utilisateur régulier du système.

Pour définir les opérateurs:

1. Dans l'arborescence, sélectionnez l'élément **Opérateurs.**



2. Dans la barre d'outils, cliquez sur l'icône 



3. Dans le champ **ID**, entrez le nom de l'opérateur.

4. **Déconnexion automatique** (**Auto Logout**) - pour définir le temps en minutes durant lequel le client AxTraxPro se déconnectera.

5. Cliquez sur **Enable** (Activer) pour activer cet opérateur.

6. Sélectionnez **Localize guard** pour définir l'opérateur avec des droits limités.

7. Cliquez sur **Réseaux (Networks)**... et **Cartes d'état (Status Maps)**... pour définir les droits locaux de l'opérateur associé.

8. Cliquez sur **Client Web** pour activer cette option.

9. Définissez les autorisations globales de l'opérateur pour chacun des écrans de la **liste des emplacements**.

10. Cliquez sur Mot de passe (**Password)…** pour ouvrir la boîte de dialogue Mot de passe de l'opérateur (**Operator Password)**.

11. Entrez le mot de passe de l'utilisateur dans le champ **Mot de passe** et entrez à nouveau le mot de passe dans le champ Confirmer le mot de passe.

Lors de la première utilisation, laissez le champ du mot de passe vide et entrez (et confirmez) votre nouveau mot de passe.

12. Cliquez sur **OK** pour enregistrer vos paramètres.

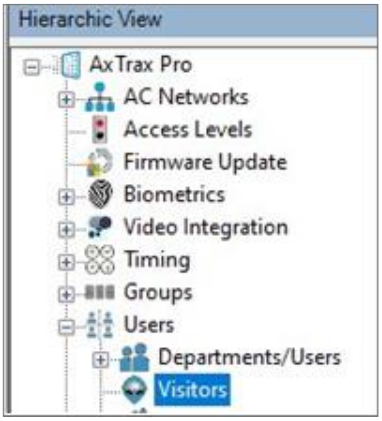
La boîte de dialogue se ferme et l'opérateur apparaît dans la zone d'affichage.

12. Gestion des visiteurs

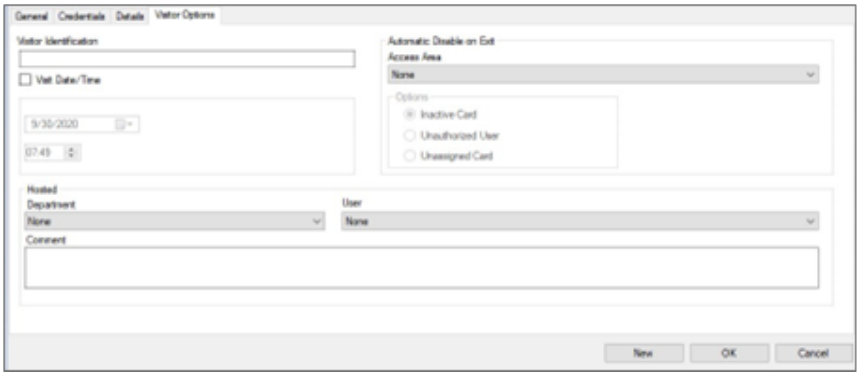
Outre les utilisateurs réguliers, vous pouvez également ajouter des visiteurs au système, y compris leurs coordonnées, les détails de la carte associée et les droits d'accès.

Pour créer des visiteurs:

1. Dans l'arborescence **Utilisateurs**, cliquez sur Visiteurs.



2. Cliquez sur l'icône 
3. Pour définir les propriétés générales, les informations d'identification et les détails, utilisez la même procédure que pour ajouter un utilisateur, voir **Ajouter un utilisateur individuel**.
4. Pour sélectionner les options du visiteur, cliquez sur l'onglet **Options du visiteur**.



Les visiteurs peuvent être présentés sous la forme d'une liste ou d'un groupe de cartes.

Pour voir les visiteurs dans une liste:

1. Cliquez sur l'icône liste 

Pour voir les visiteurs sous la forme d'un groupe de cartes:

1. Cliquez sur l'icône **Card**. 

13. Intégration des systèmes vidéo

Des caméras peuvent être ajoutées au réseau pour visualiser n'importe quelle zone en temps réel.

L'intégration vidéo peut se faire avec des serveurs Hikvision ou Dahua.

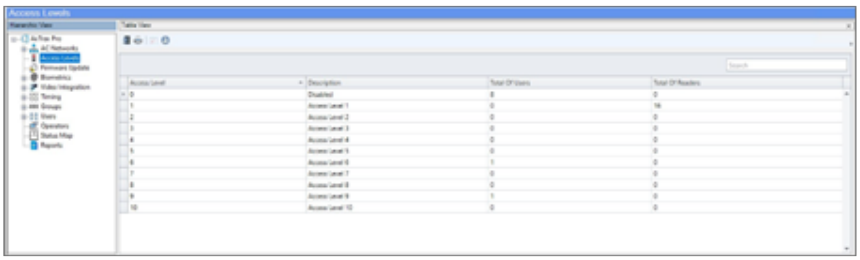
Cette fonctionnalité sera abordée dans les prochaines versions du manuel.

14. Configuration des niveaux d'accès

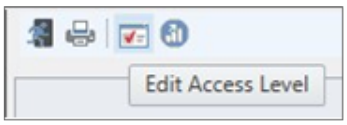
Des niveaux d'accès peuvent être attribués aux utilisateurs et aux lecteurs. Par exemple, des niveaux de sécurité différents peuvent être attribués à différentes zones d'accès et seuls certains utilisateurs y ont accès.

Un utilisateur ne peut accéder qu'à un lecteur dont le niveau d'accès est égal ou inférieur au sien dans la hiérarchie des niveaux d'accès.

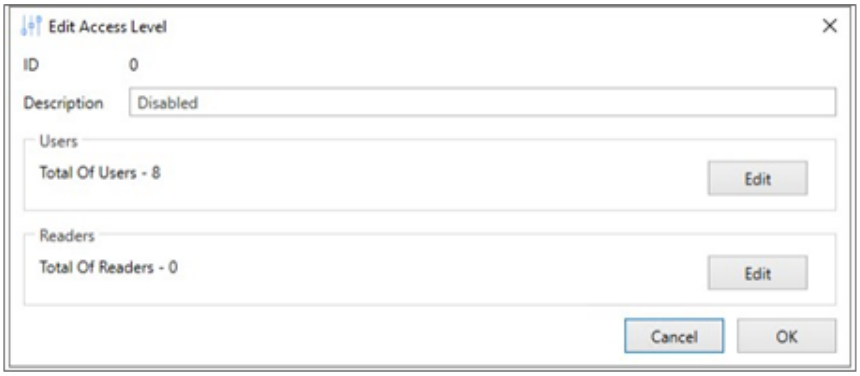
1. Dans l'arborescence, sélectionnez Niveaux d'accès (**Access Levels)**.



Sélectionnez le niveau d'accès à modifier et cliquez sur l'icône

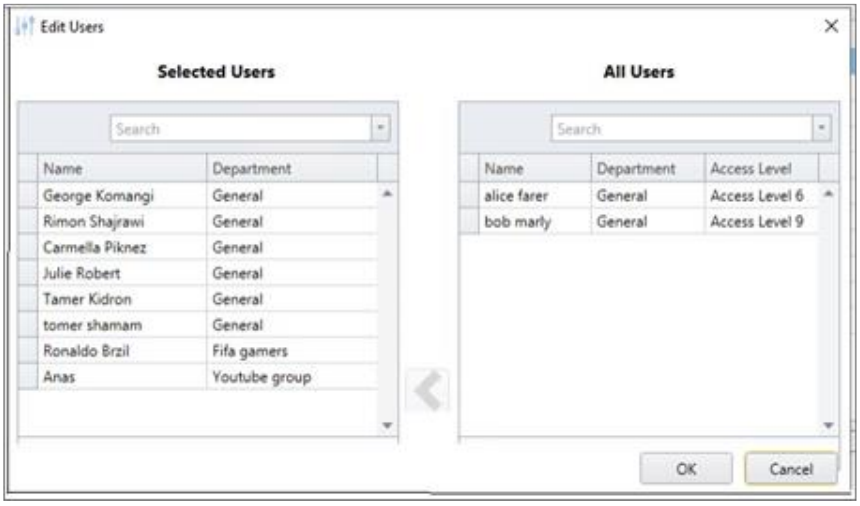


3. Pour ajouter des utilisateurs, cliquez sur Modifier (**Edit)** ans la boîte Utilisateurs (**Users)**.



Les utilisateurs peuvent également être ajoutés via l'onglet Général (**General)** de la fenêtre Propriétés de l'utilisateur (**User Properties**).

4. Pour ajouter des utilisateurs, sélectionnez les utilisateurs dans le tableau de droite et cliquez sur la flèche pour les déplacer dans la liste de gauche.

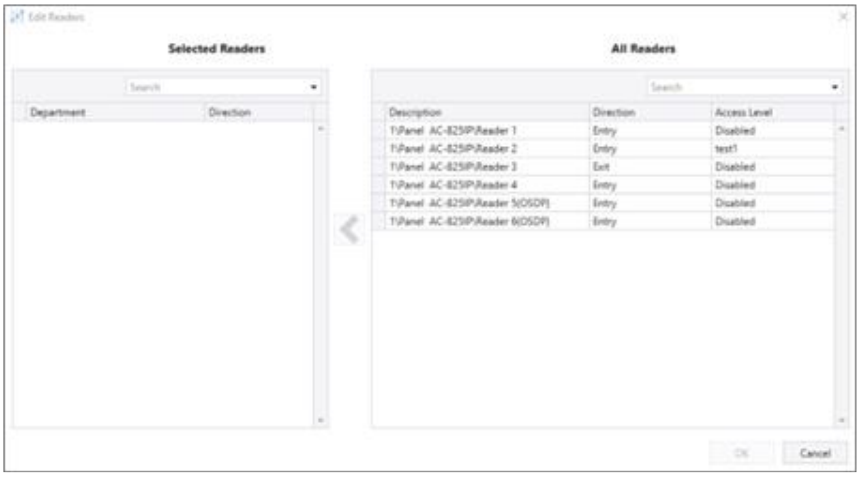


Les utilisateurs ne peuvent être supprimés que via l'onglet Général (**General)** de la fenêtre Propriétés de l'utilisateur (**User Properties)**.

5. Pour ajouter des lecteurs, cliquez sur Modifier (**Edit)** dans la boîte des lecteurs (**Readers)**.

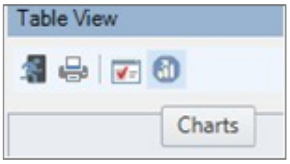
Les lecteurs peuvent également être ajoutés à partir de l'onglet Général (**General)** in de la fenêtre Propriétés du panneau (**Panel Properties)** du lecteur.

6. Pour ajouter des lecteurs, sélectionnez les lecteurs dans le tableau de droite et cliquez sur la flèche pour les déplacer dans la liste de gauche.

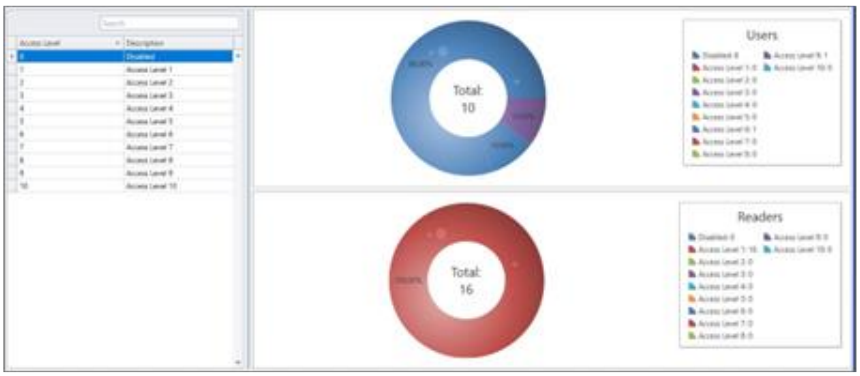


Les lecteurs ne peuvent être supprimés que via l'onglet Général (**General)** de la fenêtre Propriétés du panneau (**Panel Properties)** pour le lecteur.

8. our afficher un graphique pour les utilisateurs et les lecteurs, cliquez sur l'icône.



Pour fermer le graphique, cliquez sur l'icône



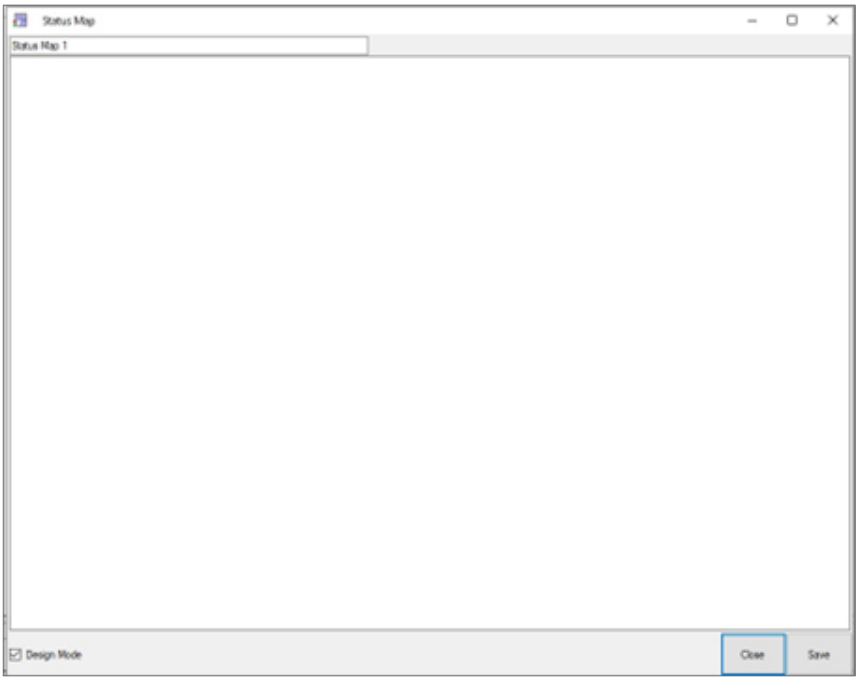
15. Création de dossiers d'état (Status Map)

Le dossier d'état affiche l'état de chaque porte, entrée et sortie, des règles AntiPassBack et des alarmes dans l'installation sur des plans d'étage sélectionnés par l'utilisateur.

Pour configurer un dossier d'état:

1. Dans l'arborescence, sélectionnez plan d'étage (**Status Map)**.

Dans la barre d'outils, cliquez sur l'icône 

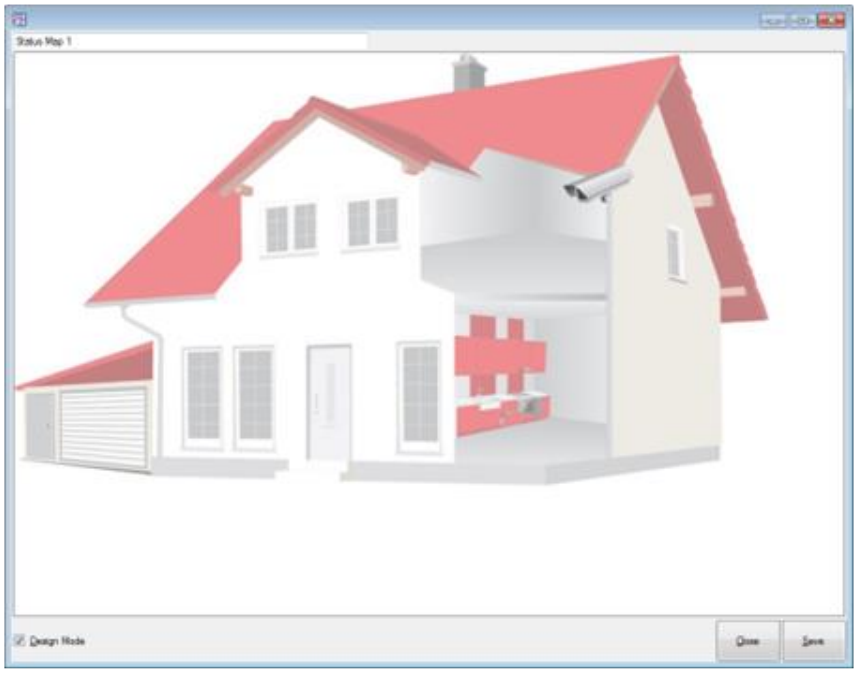


2. Cliquez avec le bouton droit de la souris dans la fenêtre et sélectionnez Définir la configuration de l'arrière-plan (**Set background)** dans le menu contextuel**.**

Pour modifier l'image de la carte et/ou ajouter des objets sur la carte, sélectionnez le mode Conception (**Design Mode).** L'icône Ajouter une plan d'étage (**Add Map)** dans la barre d'outils est activée.

4. Sélectionnez un fichier graphique (bmp, jpg, gif ou tiff) pour l'arrière-plan de la carte des statuts.

> Les icônes de plan d'étage peuvent également être ajoutées à d'autres plans d'étage pour indiquer où les deux zones de plan d'étage se touchent.



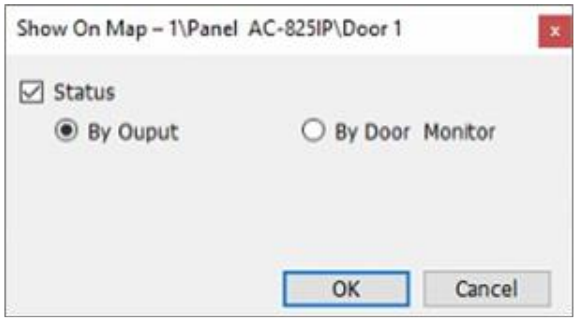
5. Assurez-vous que l'option Mode de conception (**Design Mode)** est cochée.

6. Dans l'arborescence, sélectionnez des lecteurs, des portes, des entrées, des sorties, des cartes d'état supplémentaires, des caméras ou des panneaux et cliquez sur l'icône Ajouter au plan d'étage (**Add to Map)** dans le menu de la barre d'outils.

   Les objets apparaissent dans le plan d'étage et peuvent être déplacés à l'endroit approprié.

7. Cliquez avec le bouton droit de la souris sur un objet cartographique et sélectionnez Afficher sur la carte (**Show on Map)** dans le menu contextuel.

8. Sélectionnez État (**Status)** pour afficher l'état de l'objet sur la carte d'état.



9. Pour l'option Afficher sur la carte les propriétés d'une porte, sélectionnez:

   a. **By Door Monitor (Par moniteur de porte)**: affiche les portes ouvertes en fonction de leur position physique..

   b. **By Output (Par sortie):** affiche l'état d'ouverture des portes en fonction de l'état de leur serrure.

10. Sélectionnez **Alarme** pour activer une alarme visuelle sur la carte en cas d'alarme..

> L'option d'alarme n'est disponible que pour les éléments de panneau où l'alarme a déjà été définie (voir **le champ Générer une alarme dans le tableau de la section Ajout de liens de panneau**).

11. Répéter les étapes 6 à 10 si nécessaire.

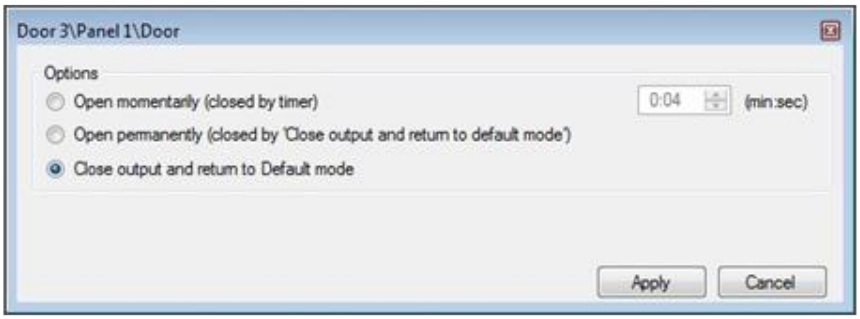
12. Répétez les étapes 1 à 10 pour configurer d'autres cartes d'état.

15.1. Ouverture manuelle d'une porte à partir de la carte des états

Vous pouvez ouvrir manuellement une porte à partir de la carte des états.

Pour ouvrir manuellement une porte à partir de la carte des états:

1. Désactivez le mode Conception (**Design Mode)** dans le coin inférieur gauche de la carte des états.



Les options disponibles sont les mêmes que celles décrites dans la section **Contrôle manuel de la porte.**

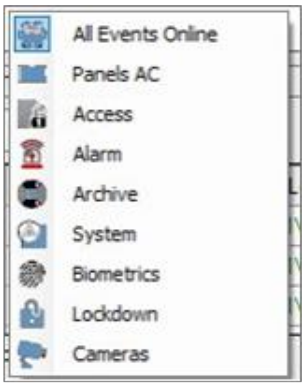
3. Sous **Options**, sélectionnez l'option souhaité.
4. Cliquez sur Appliquer (**Apply)**.

16. Visualiser les événements

Pour visualiser les événements:

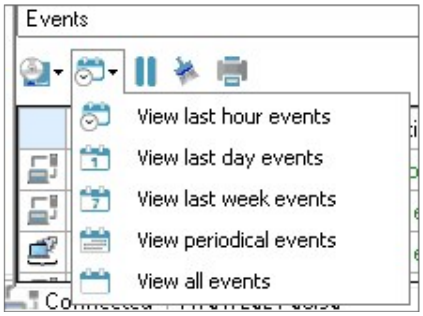
1. Dans la fenêtre Événements, sélectionnez l'icône.

2. Cliquez sur une icône pour afficher sa liste d'événements. Les options sont présentées ci-dessous.



3. Pour sélectionner une période dans la liste des événements, cliquez sur l'icône Événements.

4. Sélectionnez une tranche horaire.



17. Visualisation des rapports

AxTraxPro peut générer différents rapports, y compris des rapports d'utilisation, des enregistrements de présence, des visiteurs et des appels de rôle. L'assistant de rapports AxTraxPro permet aux utilisateurs de concevoir leurs propres rapports personnalisés en fonction de leurs besoins.

Pour plus d'informations:

17.1. Générer un rapport

Pour générer un rapport:

1. Dans l'arborescence, sélectionnez l'élément **Rapports.**
2. Sélectionnez l'une des quatre catégories de rapport principales.

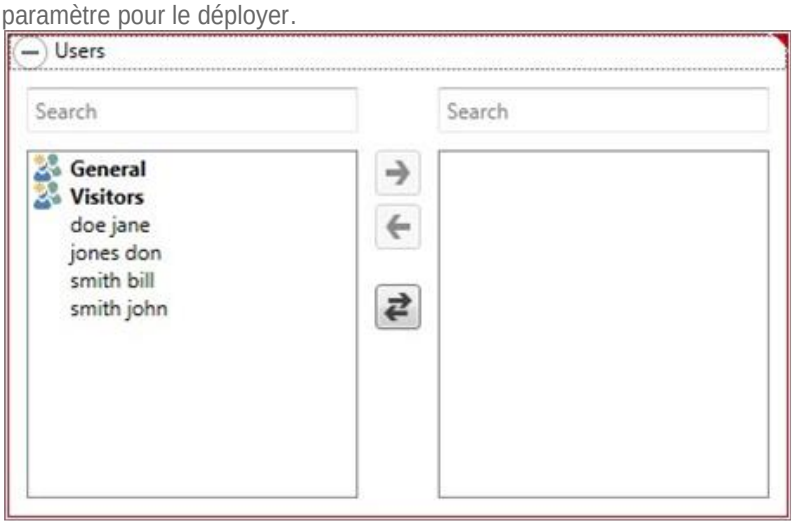
3. Sélectionnez un type de rapport dans cette catégorie:

   En fonction de la catégorie et du type de rapport sélectionnés, les paramètres appropriés apparaissent dans la zone d'affichage.

   Par exemple, les paramètres requis pour le rapport sur les droits de l'utilisateur sont affichés.

Un paramètre en rouge doit être sélectionné, alors que les paramètres qui ne sont pas en rouge sont optionnels.

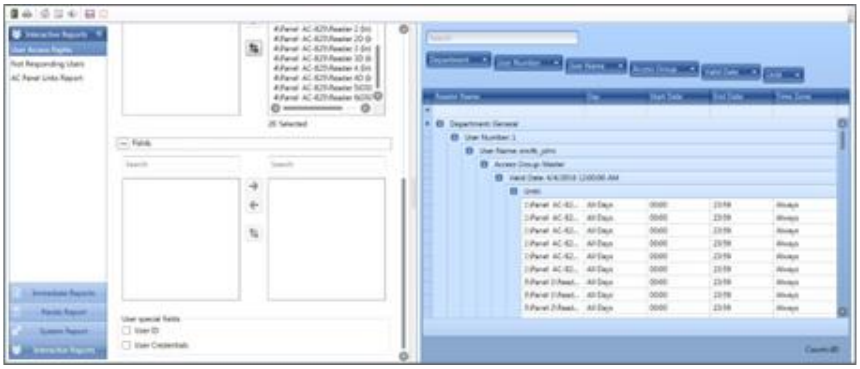
4. Cliquez sur un paramètre pour le déployer.



5. Sélectionnez et déplacez les entités souhaitées à l'aide des flèches.

6. Une fois que toutes les entités de chaque paramètre sont sélectionnées, cliquez sur l'icône de la barre d'outils pour générer un rapport.

Le rapport généré, dans cet exemple le rapport sur les droits d'accès des utilisateurs, apparaît dans la zone d'affichage.

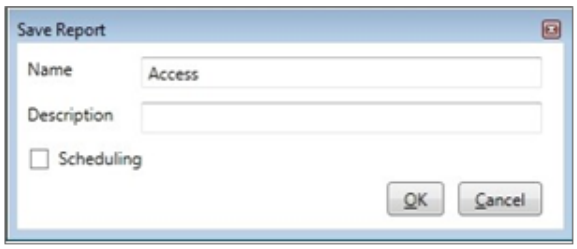


17.2. Planification d'un rapport

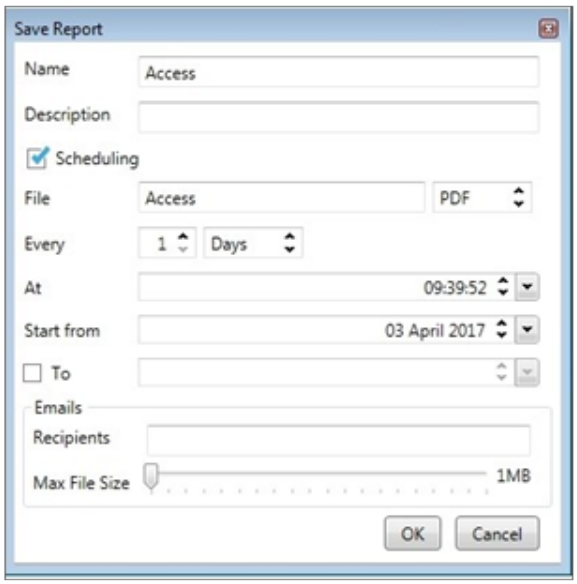
Lorsque vous avez généré un rapport pour la première fois, vous pouvez programmer le même rapport pour qu'il soit automatiquement généré et sauvegardé à l'heure de votre choix.

Pour planifier un rapport:

1. Lorsque le rapport généré apparaît dans la zone d'affichage, cliquez sur l'icône dans la barre d'outils



2. Entrez le nom et la description du rapport planifié
3. Sélectionnez Planification (**Scheduling)** pour déployer les options.



4. Dans les champs disponibles, définissez les paramètres (format, intervalle, période, destinataires des emails) pour le rapport programmé à générer.

Pour utiliser les notifications par e-mail, configurez les paramètres SMTP (voir **Paramètres de notification**).

5. Cliquer sur **OK**.

Le rapport enregistré apparaît dans la zone d'affichage.

Pour ouvrir à tout moment la liste des rapports programmés enregistrés, cliquez sur l'icône dans la barre d'outils.

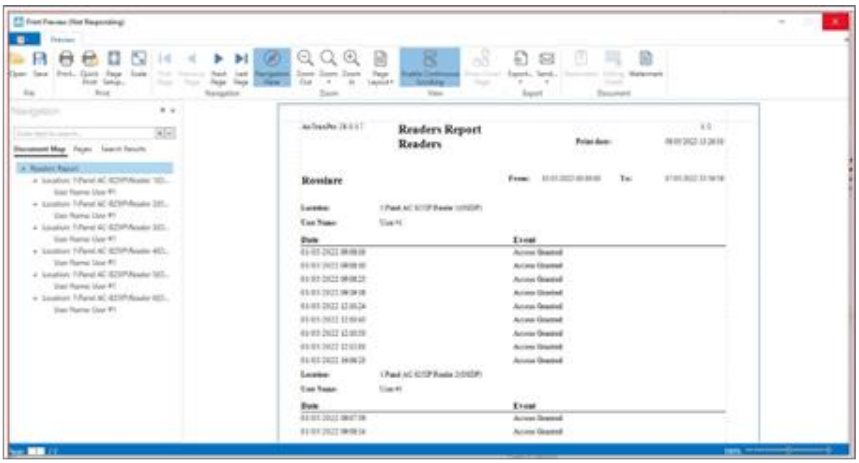
Pour supprimer un rapport programmé, sélectionnez-le dans la zone de visualisation et cliquez sur l'icône de la barre d'outils.

17.3. Visualisation d'un rapport

Vous pouvez visualiser un rapport généré avant de l'enregistrer ou de l'imprimer.

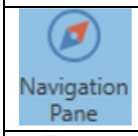
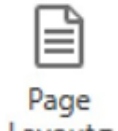
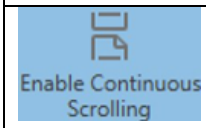
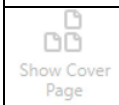
Pour visualiser un rapport:

1. Dans la barre d'outils, cliquez sur l'icône pour afficher le rapport.



Les icônes disponibles pour chaque type d'aperçu de rapport sont décrites dans le tableau suivant:

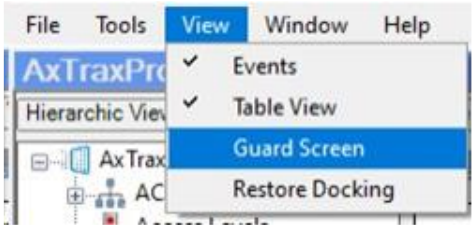
Icône	Nom	Cliquer sur le bouton pour .....
Open	Ouvrir	Ouvrir un rapport déjà enregistré
Save	Sauvegarder	Sauvegarder le document du rapport
Print...	Imprimer	Imprimer avec des paramètres personnalisables

Icône	Nom	Cliquer sur le bouton pour….
	Quick Print	Impression du document avec les paramètres par défaut
	Page Setup	Personnaliser les paramètres du document
	Scale	Ajuster l'échelle de la page
	Navigation Pane	Ouvre le panneau de navigation pour naviguer dans un document et rechercher du texte.
	Zoom Out	Pour voir plus de la page
	Zoom	Utilisé pour voir plus de détails.
	Zoom In	Zoom pour agrandir le texte sur la page
	Page Lay-out	Permet de sélectionner une page du document: - Page unique - Affiche une page de document à la fois.. - Deux pages - Affiche deux pages de document côte à côte. - Wrap Pages - Affiche les pages côte à côte (le facteur de zoom actuel limite le nombre de pages côte à côte).
	Enable continuous Scrolling	Spécifie s'il faut sauter au début de la page suivante lorsque la fin de la page précédente est atteinte ou activer le défilement vertical continu.  Cette commande ne peut être sélectionnée que lorsque la mise en page est réglée sur Une page ou Deux pages.
	Show Cover Page	Spécifie si la première page du document doit être affichée séparément ou à côté de la page suivante.  Cette commande n'est activée que lorsque la mise en page est définie sur Deux pages.
	Export document	Utilisez la flèche de droite pour choisir le format dans lequel vous souhaitez exporter le document.
	Send via email	Utilisez la flèche de droite pour choisir le format dans lequel vous souhaitez enregistrer le document et l'envoyer par e-mail.
	Editing Fields	Mettez en surbrillance les champs permettant d'éditer le document.

18. Visualisation de l'écran de garde

Pour afficher l'écran de garde:

1. Dans la barre de menus, sélectionnez **View > Guard Screen**.



L'écran de garde suivant s'affiche.

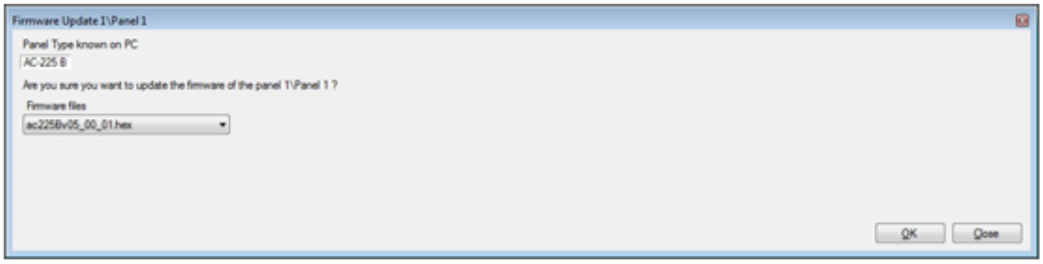
19. Mise à jour du micrologiciel

La fenêtre Mise à jour du micrologiciel permet à un opérateur de mettre à jour la version du micrologiciel de la centrale de contrôle d'accès sélectionnée. Pour les panneaux AC-825IP, vous pouvez également mettre à jour le micrologiciel des extensions connectées.

19.1. Panneaux AC-215x, AC-225x et AC-425x

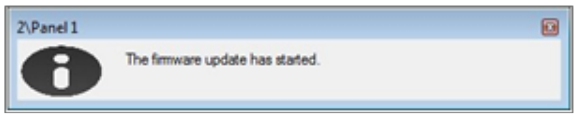
Pour mettre à jour le micrologiciel:

1. Dans l'arborescence, développez l'élément **AC Networks** et développez un réseau sélectionné..
2. Sélectionnez un panneau.
3. Dans la barre d'outils, cliquez sur l'icône 

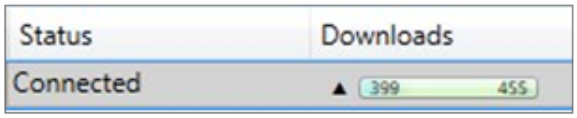


4. Dans la liste déroulante, sélectionnez le fichier HEX correspondant au type de matériel du panneau.
5. Cliquez sur **OK.**

   En bas de l'écran, une barre de progression s'affiche jusqu'à ce que la mise à jour du micrologiciel soit trouvée, puis une fenêtre contextuelle apparaît pour indiquer que la mise à jour a commencé.



6. Pour connaître la progression de la mise à jour, sélectionnez le réseau dans l'arborescence et consultez la colonne **Téléchargements** dans la **zone d'affichage.**



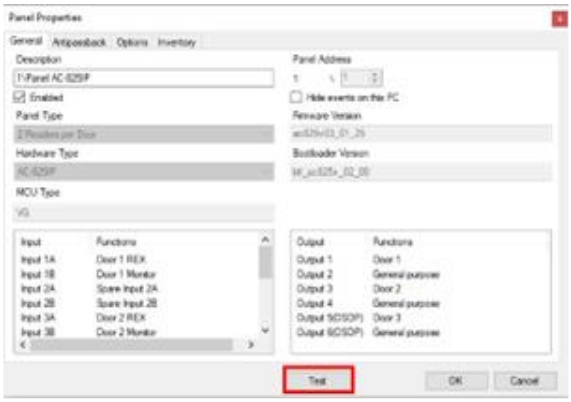
   La mise à jour est terminée lorsque le nombre de téléchargements tombe à zéro n'apparaît plus dans la colonne. Le statut du panneau est maintenant "**Connected**".

19.2. Panneau AC-825IPP

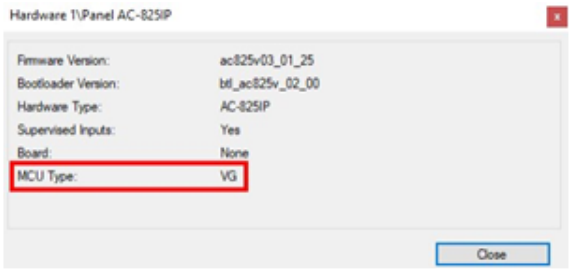
La procédure de mise à jour du micrologiciel suivante ne s'applique qu'à un panneau AC-825IP avec un type de contrôleur **VG MCU**.

Pour vérifier le type de contrôleur MCU:

1. Dans **l'arborescence**, développez l'élément **AC Networks** et développez le réseau sélectionné.
2. Sélectionnez le panneau AC-825IP.
3. Cliquez sur **Test.**



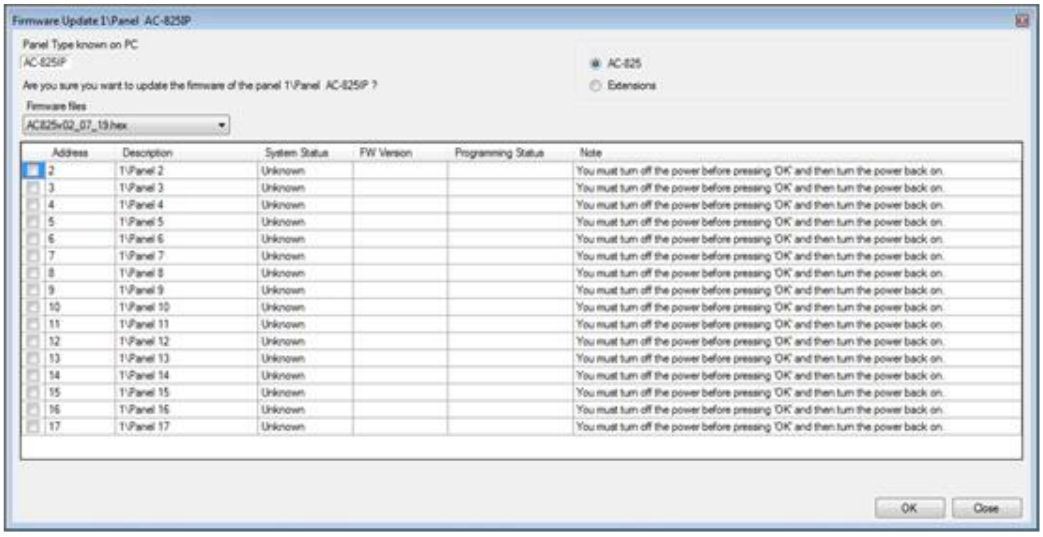
4. Vérifiez que le type de contrôleur MCU est **VG**.



Pour mettre à jour le micrologiciel:

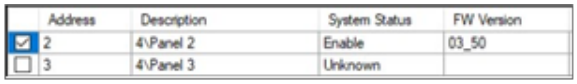
1. Dans l'arborescence, développez l'élément **AC Networks** et développez le réseau sélectionné..
2. Sélectionnez un panneau.
3. Dans la barre d'outils, cliquez sur l'icône 

La fenêtre **Firmware Update** (Mise à jour du micrologiciel) s'ouvre.



4. Par défaut, le panneau principal est sélectionné pour être mis à jour.

5. Dans la liste déroulante, sélectionnez le fichier HEX correspondant au type de périphérique du panneau.
6. Si vous sélectionnez **Extensions** pour mettre à jour le micrologiciel d'une extension, vous devez également sélectionner l'extension à mettre à jour.

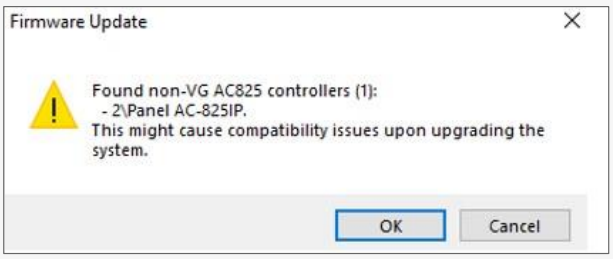


Vous ne pouvez sélectionner qu'un seul panneau à mettre à jour.

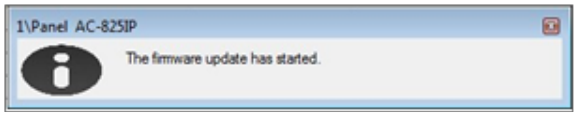
7. Cliquer sur **OK**.

Le message suivant s'affiche si l'AC-825IP est de type **VC MCU.**

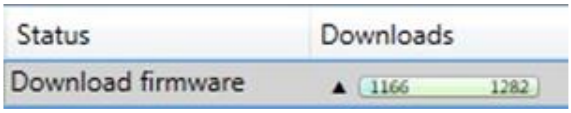
Le message suivant s'affiche si l'AC-825IP n'est pas un **VG MCU** ou **VC MCU**



Une barre de progression s'affiche en bas de l'écran jusqu'à ce que la mise à jour du micrologiciel soit trouvée, puis une fenêtre contextuelle apparaît pour indiquer que la mise à jour a commencé.



8. Pour voir la progression de la mise à jour, sélectionnez le réseau dans l'arborescence et observez la colonne Téléchargements dans la zone d'affichage.

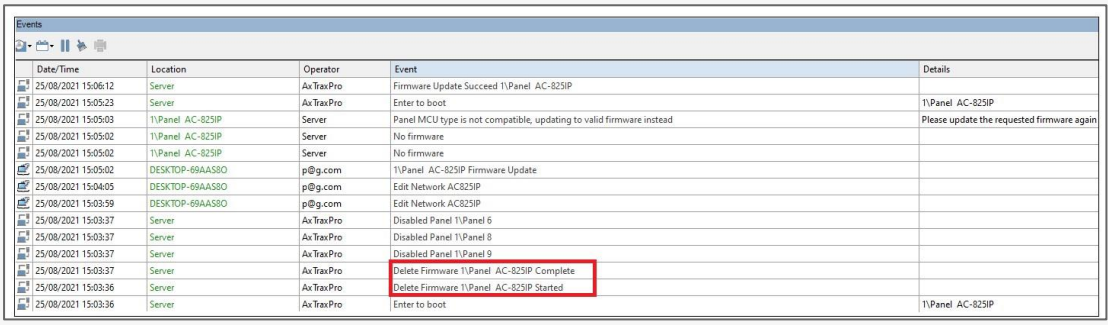


La mise à jour est terminée lorsque le nombre de téléchargements tombe à zéro et n'apparaît plus dans la colonne. Le statut du panneau est maintenant "Connecté" (**Connected**).

Pour effacer le micrologiciel:

1. Dans l'arborescence, développez l'élément **AC Networks** (Réseaux CA) et développez un réseau sélectionné.
2. Sélectionnez un panneau.
3. Dans la barre d'outils, cliquez sur l'icône 

Une fois le microprogramme supprimé, le journal des événements affiche le message suivant:



Annexe A. Opérations de l'administrateur système

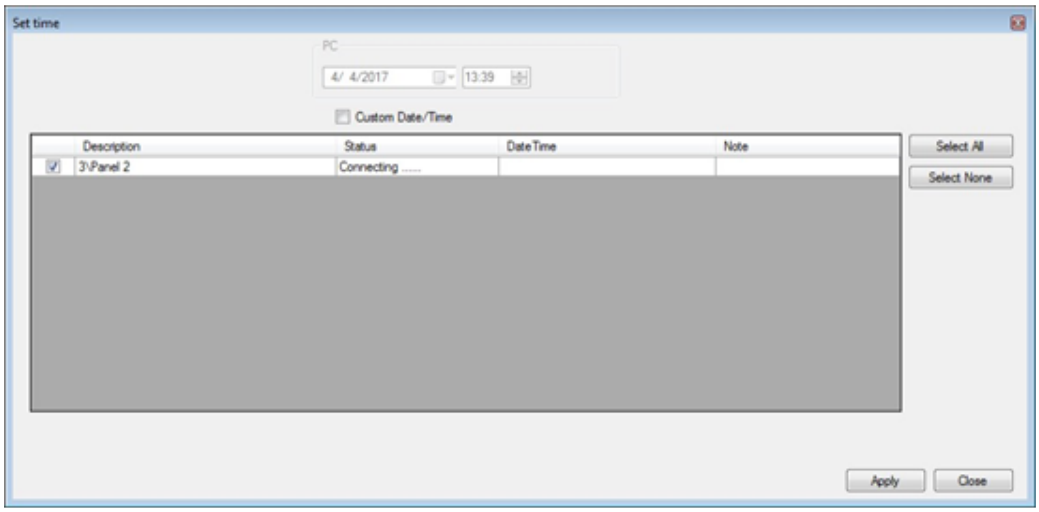
A.1 Paramétrage de la date et de l'heure

La fenêtre **Set Time** permet de sélectionner les panneaux par réseau et de réinitialiser leur date et leur heure en fonction de la date et de l'heure du système du serveur AxTraxPro.

Pour réinitialiser l'heure du panneau:

1. Dans **l'arborescenc**e, développez l'élément **AC Networks** et sélectionnez un réseau.

2. dans la barre d'outils, cliquez sur l'icône 



3. Sélectionnez les panneaux à réinitialiser.
4. Cliquer sur **Apply**.

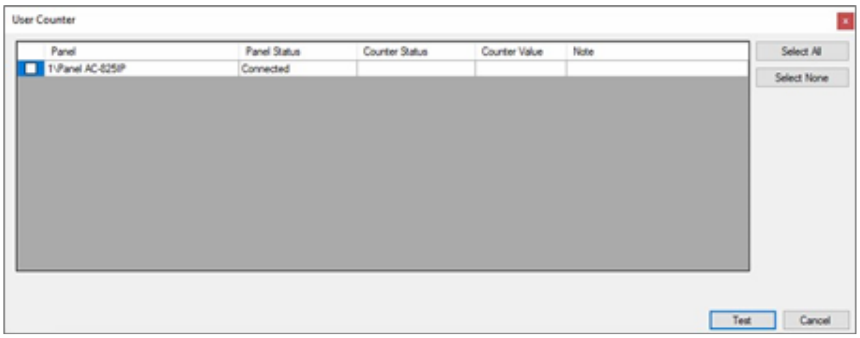
   Le serveur se connecte aux panneaux et modifie l'heure comme demandé. Une boîte de dialogue confirme l'opération.

A.2 Test des compteurs d'utilisateurs

Lors de l'utilisation des compteurs d'utilisateurs, il est possible de visualiser la valeur actuelle du nombre d'utilisateurs dans chaque panneau avec un lecteur désigné par l'option "Déduire le compteur d'utilisateurs" (**Deduct User Counter**).

Pour visualiser les compteurs d'utilisateurs:

1. Dans l'arborescence, développez l'élément **Utilisateurs.**
2. Sélectionnez l'élément **Visiteurs** ou développez l'élément **Département/Utilisateurs** et sélectionnez un département.
3. Sélectionnez un utilisateur ou un visiteur dans la **zone d'affichage.**
4. Dans la barre d'outils, cliquez sur l'icône 

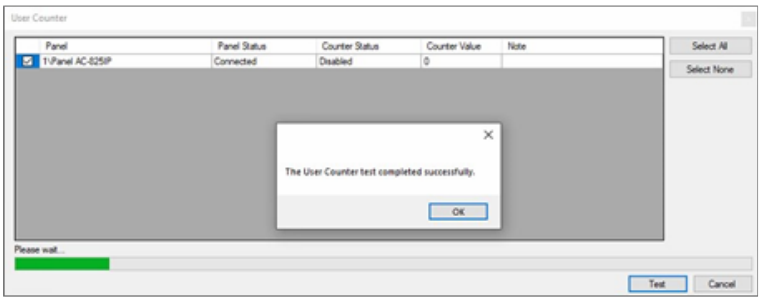


Pour qu'un panneau apparaisse dans le tableau, il doit avoir au moins un lecteur pour lequel l'option Soustraire le compteur de l'utilisateur est sélectionnée dans l'onglet Général de la fenêtre Propriétés du lecteur.

5. Sélectionnez le ou les panneaux que vous souhaitez tester.
6. Cliquer sur **Test**.

   Une barre de progression s'affiche en bas de l'écran et un message de confirmation apparaît lorsque le test est terminé.
7. Cliquer sur **OK**.

   Les champs restants du tableau sont maintenant remplis.



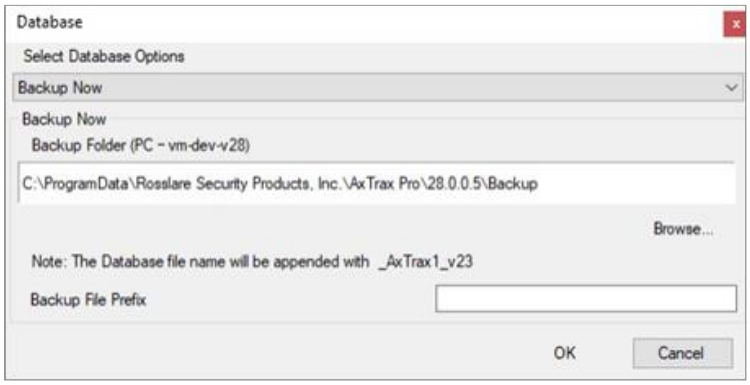
A.3 Maintenance de la base de données

Il est fortement recommandé de sauvegarder la base de données du système une fois par semaine sur un périphérique de stockage externe.

Utilisez la fenêtre Base de données pour gérer la base de données du système.

Pour ouvrir la fenêtre Base de données:

1. Dans la barre de menus, sélectionnez **Tools > Database**.



2. Dans le menu déroulant Sélectionner les **options de la base de données**, sélectionnez l'option souhaitée, comme décrit dans le tableau suivant:

Fonctionnement	Description
Sauvegarde périodique	Effectuer une sauvegarde programmée tous les jours à l'heure spécifiée.
Sauvegarde maintenant	Effectuer immédiatement une sauvegarde unique
Exporter des configurations et des événements*	Copie le contenu de la base de données dans le dossier sélectionné.
Importer des configurations*	Remplace la configuration actuelle sur la base du fichier importé. La photo d'un utilisateur peut également être importée.
Importer des configurations et des événements	Remplace la configuration et les événements actuels sur la base du fichier importé.
Supprimer des configurations et des événements*	Supprime la configuration actuelle de la base de données et tous les événements.
Limitation de la période des événements	Supprimer automatiquement les événements s'ils sont plus anciens qu'un certain nombre de jours. Avant d'utiliser cette option, Rosslare vous recommande de mettre en place un système de de sauvegarde périodique. Il est recommandé de fixer la valeur à un maximum de 91 jours.
Supprimer les événements du panneau	Supprimer tous les événements datant de plus d'un certain nombre de jours.
Importer les versions précédentes de la base de données AxTraxNG/AxTraxPro	Remplacer la base de données actuelle La photo d'un utilisateur peut également être importée
Exporter des événements de contrôle d'accès	Copier le contenu des événements de contrôle d'accès de la base de données dans le dossier sélectionné.

*Cette option n'est disponible que dans le PC AxTraxPro.

3. Cliquez sur Parcourir (**Browse)** pour rechercher le fichier à importer ou sélectionnez le dossier vers lequel vous souhaitez exporter.

Pour importer un fichier DB, le fichier doit être situé dans le dossier C:ProgramData. Il se peut que vous deviez afficher tous les fichiers cachés pour voir le dossier Program Data.

Les fonctions de sauvegarde et d'exportation ajoutent "_AxTrax1_vX" à la fin du nom du fichier de la base de données exportée ou sauvegardée. La fonction d'importation de base de données n'est exécutée qu'avec un fichier contenant cette chaîne à la fin du nom de fichier. Après l'importation d'une base de données, l'état du panneau peut devenir désactivé. Dans ce cas, l'opérateur doit réactiver les panneaux.

4. Cliquer sur **OK**.

A.4 Options et préférences pour AxTraxPro

AxTraxPro peut être personnalisé selon les préférences de l'opérateur à l'aide de la fenêtre "Options".

Pour ouvrir la fenêtre "Options":

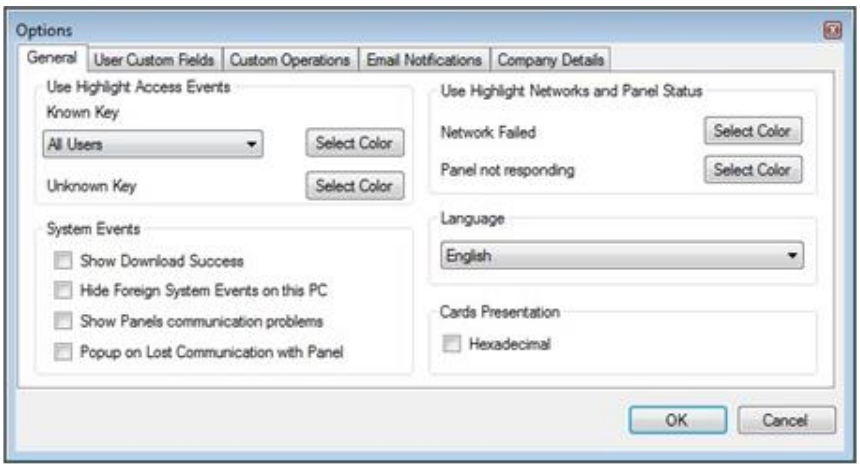
1. Dans la barre de menu, sélectionnez **Tools > Options**.

   La fenêtre **Options** contient 5 onglets:

   - **General** – Paramètres généraux de démarrage et de présentation
   - **User Custom Fields** – Champs supplémentaires définis par l'utilisateur pour la fenêtre **Propriétés de l'utilisateur**.
   - **Custom Operations** – Permet de télécharger des utilisateurs dans le système à partir d'un fichier texte.
   - **Email Notifications** – Permet d'envoyer des notifications d'événements sélectionnés à une liste de mails spécifiés.
   - **Company Details** – Détails de l'emplacement (nom et adresse) affichés dans le rapport.

A.4.1 Onglet Général

L'onglet Général contient les paramètres de la connexion de présentation.

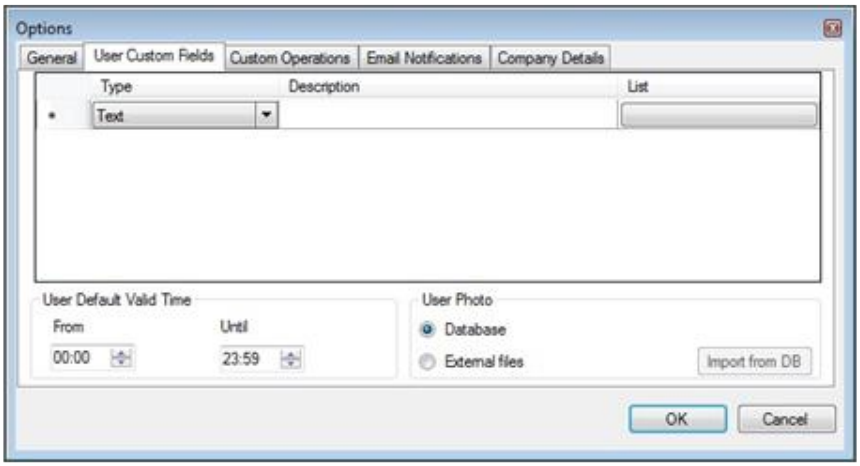


L'onglet **Général** contient les champs suivants :

Champs	Description
Utiliser les événements d'accès à la mise en évidence	Sélectionnez l'option souhaitée dans le menu déroulant **Know Key** et cliquez sur **Select** colour pour afficher les informations utilisateur sélectionnées dans une surbrillance colorée choisie par l'utilisateur lui-même (....). Cliquer sur **Select Color** à côté de **Unknown key** om pour définir la couleur de la surbrillance pour les touches inconnues.
Événements système>Montrer le succès du téléchargement	Sélectionnez cette option pour ajouter un message à l'historique des événements lorsque le téléchargement des paramètres du système depuis le logiciel AxTraxPro vers le panneau est réussi.
Événements système>Masquer les événements système étranges sur ce PC	Sélectionnez cette option pour ne voir que les messages de l'administrateur local et du serveur AxTraxPro.
Événements système>Afficher les problèmes de communication avec le panneau	Sélectionnez cette option pour que l'état indique les problèmes de communication avec le panneau
Événements système>Affichage d'une fenêtre contextuelle en cas de perte de communication avec le tableau de bord	Cochez cette case pour faire apparaître une fenêtre contextuelle en cas de perte de communication avec un panneau. Après avoir activé la case à cocher, déconnectez le panneau en fonctionnement et attendez une minute ou deux pour voir si la fenêtre contextuelle apparaît.
Utiliser Mettre en évidence les réseaux et l'état du panneau	Cliquez sur **Select Color** en regard de **Network failed** pour définir la couleur du marqueur pour les alarmes réseau. Cliquez sur **Select Color** en regard de **Panel not responding** pour définir une couleur de marquage pour les pannes de communication du panneau.
Langue	Sélectionnez la langue de l'interface du système. Le choix de la langue (Farsi) modifie également le format de la date (Farsi).
Présentation des cartes	Modifie l'affichage des données cartographiques au format hexadécimal.

A.4.2 Champs personnalisés utilisateur

L'onglet Champs personnalisés utilisateur (**User Custom Fields)** gère les champs définis par l'utilisateur dans l'onglet Général de la fenêtre Propriétés de l'utilisateur (**User Properties)**.

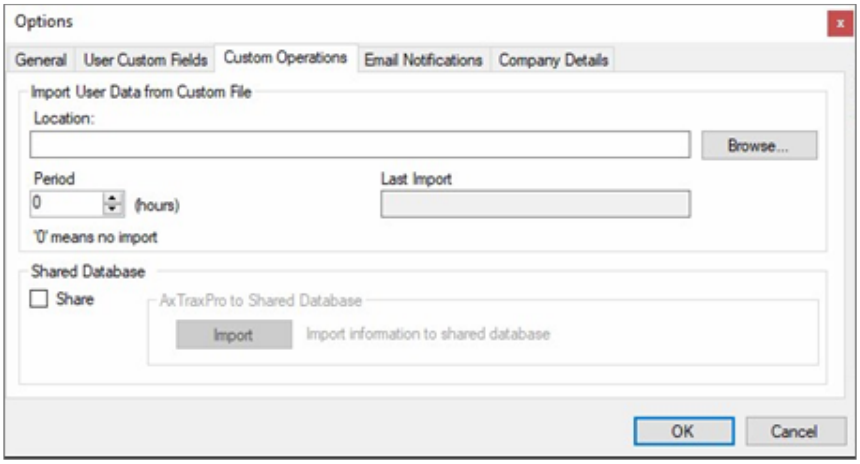


L'onglet Champs personnalisés utilisateur (**User Custom Fields)** contient les champs suivants:

Champs	Description
Type	Sélectionnez le type de champ. S'il s'agit d'une **liste**, cliquez sur **Modifier la liste** et saisissez les éléments de la liste.
Description	Entrez ici un nom pour le nouveau champ.
Liste	Un texte avec plusieurs valeurs qu'un utilisateur peut ajouter et utiliser pour sélectionner une valeur dans la liste.
Durée de validité par défaut de l'utilisateur	Définissez les heures de début et de fin par défaut pour les droits d'accès de l'utilisateur à l'aide des champs Du et Au.
Photo de l'utilisateur	Définir les photos par défaut à utiliser: • Base de données (**Database)**: utiliser les photos d'utilisateurs stockées dans la base de données • Fichiers externes (**External files):** utilisez cette option pour stocker une grande collection de photos d'utilisateurs en dehors de la base de données. • Exporter de la base de données (**Export from DB):** cliquez sur ce bouton pour exporter les photos existantes de la base de données vers un dossier externe. dossier externe.

A.4.3 Opérations personnalisées

L'onglet Opérations personnalisées (**Custom Operations)** permet de télécharger dans le système les données de l'utilisateur à partir d'un fichier texte et de définir l'option de base de données partagée.

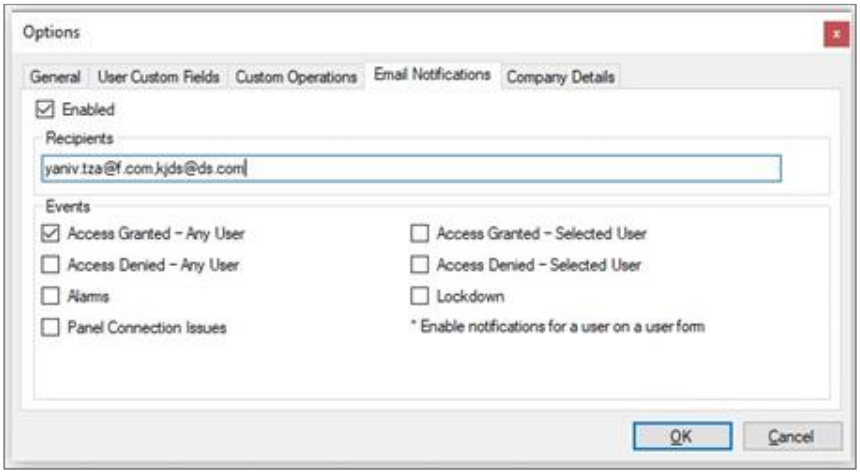


L'onglet Opérations personnalisées (**Custom Operations)** contient les champs suivants:

Champs	Description
Importation de données utilisateur à partir d'un fichier personnalisé	Met deze optie kunt u gebruikersgegevens van bezoekers importeren uit een tekstbestand (*.txt). Les données importées couvrent les champs suivants : Numéro d'utilisateur, Nom, Prénom, Date d'embauche au format jj/mm/aa, Date de validité (facultative). Les valeurs doivent être séparées par un ",". Chaque visiteur doit se trouver sur une nouvelle ligne du fichier texte. Sélectionnez l'emplacement du fichier à importer/exporter à l'aide de la fonction Parcourir (**Browse)**. Dans la case Période (**Period)** sélectionnez la période de temps. La période est le temps entre les processus d'importation en heures, où "0" signifie que l'importation est uniquement manuelle..
Importation de données utilisateur à partir d'un fichier personnalisé	Cliquez sur **Importer** pour transformer les données ci-dessus en une base de données à partir de laquelle les données peuvent être partagées par un programme externe

A.4.4 Notifications par e-mail

L'onglet Notifications par e-mail (**Email Notifications)** permet d'envoyer des notifications d'événements sélectionnés à une liste d'e-mails spécifiés.

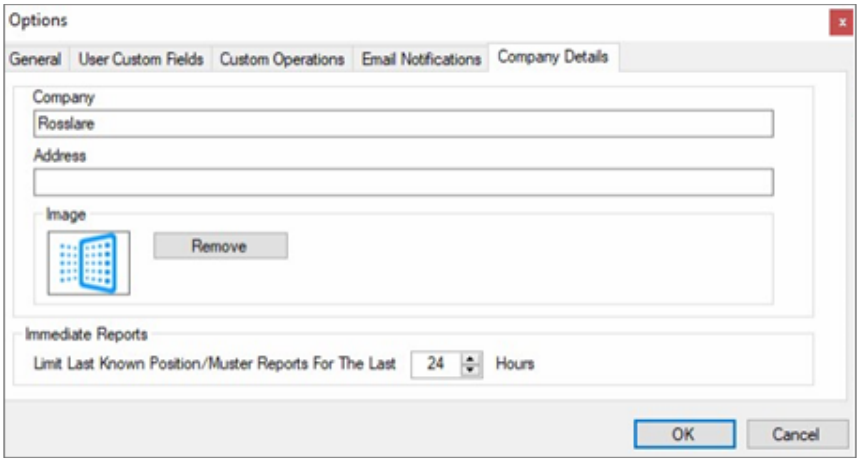


Entrez les adresses e-mail de votre/vos destinataire(s) et sélectionnez les événements pour lesquels vous souhaitez recevoir des notifications.

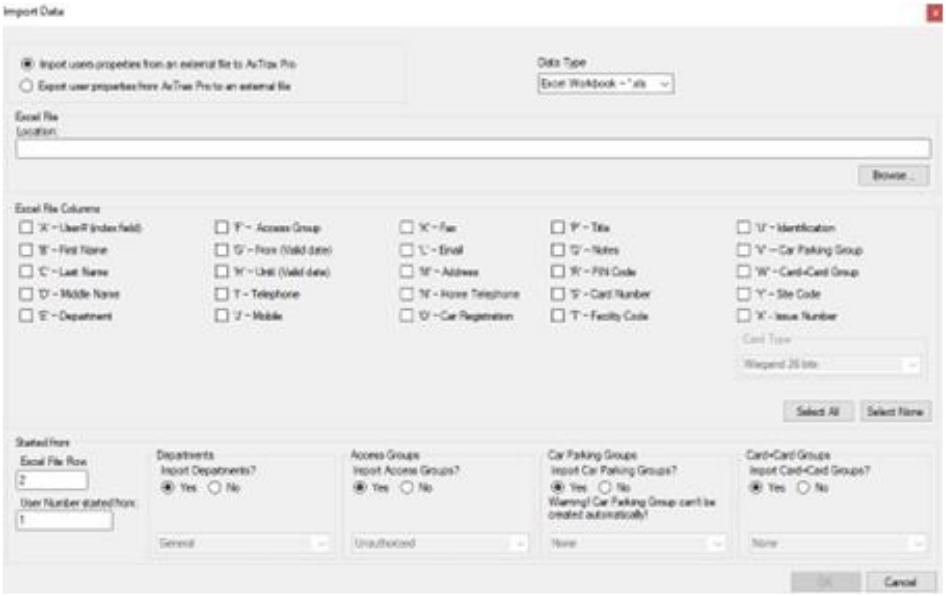
Pour utiliser les notifications par e-mail, vous devez configurer les paramètres SMTP (Paramètres de notification).

A.4.5 Détails de l'entreprise

L'onglet Détails de l'entreprise (**Company Details)** indique le nom et l'adresse affichés dans les rapports.



A.5 Importer/Exporter des données utilisateurs



La fenêtre d'importation/exportation de données (**Import/Export Data)** permet d'importer/exporter des informations sur les utilisateurs dans/depuis la base de données AxTraxPro depuis/vers un fichier tableur standard.

Pour importer/exporter des données utilisateur:

1. Dans la barre de menu, sélectionnez **Tools > Import/Export Data**.
2. Définissez les options d'importation/exportation en fonction des descriptions des champs dans le tableau suivant

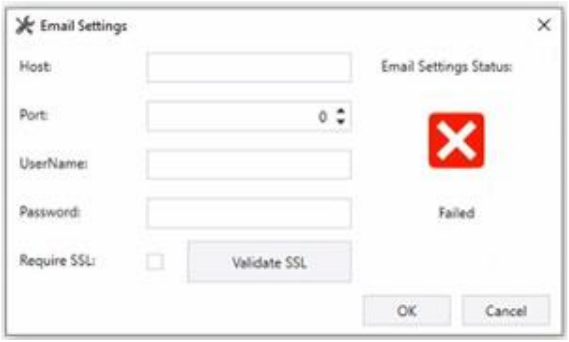
Champs	Description
Importer les propriétés d'un utilisateur dans AxTraxPro à partir d'un fichier externe	Sélectionnez cette option pour importer les propriétés de l'utilisateur
Exporter les propriétés d'un utilisateur d'AxTraxPro vers un fichier externe	Sélectionnez cette option pour exporter les propriétés des utilisateurs
Type de données	Sélectionnez le type de fichier de données à importer/exporter.
Localisation	Sélectionnez l'emplacement du fichier à importer/exporter à l'aide de la fonction Parcourir (**Browse).**
Type de données	Cochez les cases des colonnes à importer ou à exporter. Les données de chaque colonne (A-T) sont importées ou exportées comme spécifié. Lors de l'exportation du champ Notes (colonne Q), seuls les 256 premiers caractères sont inclus.
Excel-bestand Rij	Entrez la première ligne des données de l'utilisateur dans la feuille de calcul.
Gebruikersnummer gestart vanaf	Entrez le numéro à partir duquel vous commencez à attribuer des numéros d'utilisateur uniques au système.
Importeren afdelingen?	Sélectionnez Oui (**Yes)** pour importer de nouveaux départements dans la base de données AxTraxPro. Sélectionnez Non (**No)** pour importer des utilisateurs sans leur département.
Afdeling	Sélectionnez le département à attribuer aux utilisateurs importés. Cette case n'est active que si l'option **Non** est sélectionnée dans l'option Importer un département.

Champs	Description
Importation de groupes d'accès ?	Sélectionnez Oui (**Yes)** pour importer les nouveaux groupes d'accès dans la base de données AxTraxPro. Sélectionnez Non (**No)** pour ne pas importer les groupes d'accès des utilisateurs.
Groupes d'accès	Sélectionnez le groupe d'accès à attribuer aux utilisateurs importés. Cette case n'est active que si l'option **Non** est sélectionnée dans l'option Importer un groupe d'accès.
Importer des groupes de parking ?	Sélectionnez Oui (**Yes)** pour importer de nouveaux groupes de parking dans la base de données AxTraxPro. Sélectionnez Non (**No)** pour importer des utilisateurs sans leurs groupes de parking.
Groupes de parking	Sélectionnez le groupe de parking à attribuer aux utilisateurs importés. Cette case n'est active que si l'option **Non** est sélectionnée dans l'option Importer un groupe de parking.
Importer des groupes de cartes ?	Sélectionnez Oui (**Yes)** pour importer de nouveaux groupes de cartes dans la base de données AxTraxPro. Sélectionnez Non (**No)** pour importer des utilisateurs sans leurs groupes de carte+carte.
Groupes de cartes	Sélectionnez le groupe de carte+carte à attribuer aux utilisateurs importés. Cette case n'est active que lorsque l'option **Non** est sélectionnée dans l'option Importer un groupe de carte+carte.

3. Cliquer sur **OK**.

A.6 Paramètres de notification

Les paramètres de notification permettent de définir la configuration SMTP, d'afficher le dossier des notifications et de définir l'option IP statique.



Om de Notificatie Instellingen in te stellen:

1. Dans la barre de menu, sélectionnez **Tools > Notification Settings**
2. Définissez les options conformément aux descriptions des champs dans le tableau suivant:

Paramètre	Description
SMTP Settings > Host	L'adresse de votre serveur SMPT
SMTP Settings > Port	Le port de votre serveur SMPT
SMTP Settings > User Name	Le nom de compte de votre serveur SMTP
SMTP Settings > Password	Le mot de passe de votre compte
SMTP Settings > Require SSL	Cochez si votre serveur SMTP doit être sécurisé
SMTP Settings > Email Validation	Cliquez pour valider les paramètres SMTP
Report Directory	L'emplacement par défaut des rapports à générer automatiquement et à sauvegarder selon la planification (voir Planification d'un rapport) (Scheduling a Report).
IP Address > Use Static IP	Cochez Utiliser une adresse IP statique (**Use Static IP)** pour entrer une adresse IP statique. Le serveur communique avec les clients par l'intermédiaire d'une technologie à distance. Par défaut, l'adresse IP du serveur est 127.0.0.1. Si le PC utilise simultanément plusieurs cartes réseau ou réseaux virtuels, la communication à distance peut s'avérer problématique.

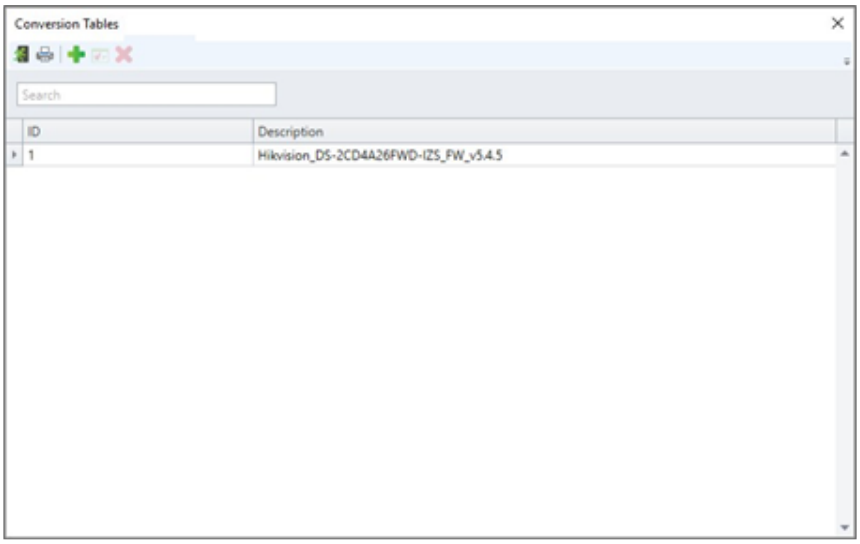
3. Cliquer sur **OK**.

A.7 Tables de conversion

Une table de conversion permet de convertir le caractère alphanumérique d'un badge en un nombre binaire qui peut ensuite être compris par le lecteur concerné en tant qu'entrée Wiegand.

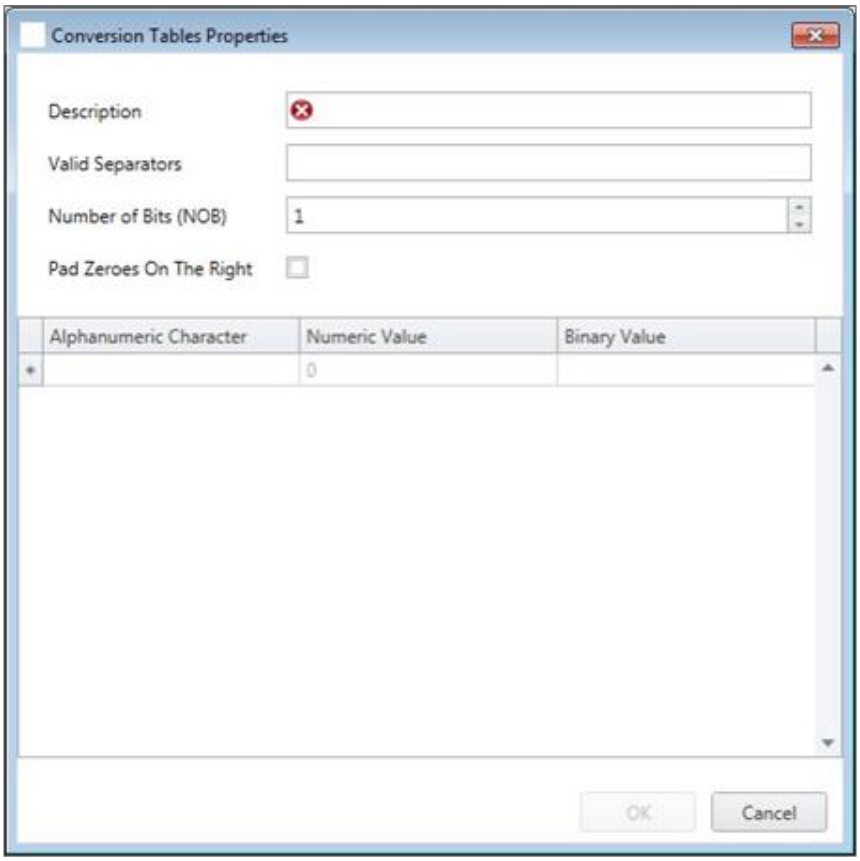
Pour créer une table de conversion :

1. Dans la barre de menu, sélectionnez **Tools > Conversion Tables**.



2. Dans la barre d'outils, cliquez sur l'icône 

   La fenêtre se ferme et la nouvelle table de conversion apparaît dans la **zone d'affichage.**



3. Définissez les options de la table de conversion en fonction des descriptions des champs dans le tableau suivant:

Champs	Description
Description	Le nom de la table de conversion
Valid Separators	Entrez le séparateur qui se trouve sur la plaque d'immatriculation Un exemple typique est "-".
Number of Bits (NOB)	Entrez le nombre de bits utilisés par chaque caractère alphanumérique.
Pad Zeroes on the Right	Vérifier que les bits non utilisés dans le format Wiegand choisi sont remplacés par des zéros à droite du code Wiegand.
Alphanumeric Character	Le caractère alphanumérique affiché sur la plaque d'immatriculation
Numeric Value	la valeur numérique attribuée au caractère alphanumérique ci-dessus
Binary Value	la valeur binaire attribuée au caractère alphanumérique ci-dessus

4. Cliquer sur **OK**.

Annexe B : Configuration d'un réseau

Le serveur AxTraxPro se connecte aux unités de contrôle d'accès via une connexion sérielle et une connexion TCP/IP.

B.1 Connexion TCP/IP

Pour connecter les panneaux de contrôle d'accès à AxTraxPro via un réseau TCP/IP LAN ou WAN, l'utilisation d'un convertisseur TCP/IP vers série est nécessaire, sauf si le panneau possède une connexion TCP-IP intégrée (AC-225IP).

Chaque connexion TCP/IP peut supporter un maximum de plusieurs panneaux de contrôle d'accès connectés via RS-485 (un maximum de 32 panneaux AC-215, AC-215IP, AC-225 ou AC-425, ou un maximum de 12 extensions avec le panneau AC-825IP).

Le câble RS-485 recommandé est une paire torsadée blindée (22 AWG).

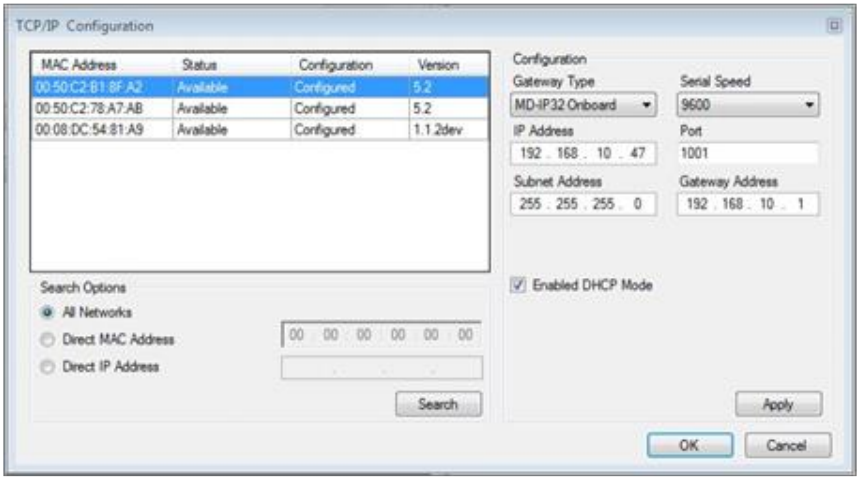
Le matériel utilisé pour se connecter au réseau TCP/IP peut être le MD-N32, qui est un convertisseur série vers Ethernet, ou le convertisseur intégré de l'AC-225IP.

Pour configurer une connexion TCP/IP à un réseau:

1. Dans l'arborescence, cliquez sur **Réseaux AC.**
2. Dans la barre d'outils, cliquez sur l'icône 
3. Définissez le type de réseau comme **TCP/IP**.

Si vous souhaitez travailler à distance, sélectionnez **Remote (WAN**) dans la fenêtre TCP/IP Network, et ajoutez l'adresse IP WAN du PC..

4. Cliquer sur **Configuration**.



La fenêtre en haut à gauche montre tous les convertisseurs TCP/IP connectés au réseau

local, identifiés par leur adresse MAC, et indique s'ils ont été précédemment assignés à un réseau ou non.

5. Sélectionnez l'adresse MAC correcte dans la liste MD-N32 (l'adresse MAC du MD-N32 doit figurer sur le convertisseur TCP/IP).
6. Sous **Gateway Type**, sélectionnez le type de convertisseur TCP/IP (MD-N32, MD-IP32 Onboard ou autre option valide).

   Pour un panneau AC-825IP, le module IP doit être configuré sur le serveur AxTraxPro. Même si le module IP a été configuré précédemment, vous devez cliquer sur Appliquer pour configurer avec le serveur et ensuite cliquer sur OK pour ajouter le réseau AC-825IP.
7. Entrez l'adresse IP et l'adresse de sous-réseau du réseau de l'ordinateur.
8. Sélectionnez la vitesse série de votre connexion et entrez le numéro de port. Il est recommandé de sélectionner un numéro de port avec une valeur plus élevée (4001 ou plus). Notez que le numéro sélectionné ne doit pas se terminer par des zéros (préférez une valeur de port de 4243 plutôt que 4200). Cela permet d'éviter les collisions avec les adresses de port réservées à différents équipements installés sur le même réseau.
9. Entrez l'adresse de la passerelle par défaut du réseau de l'ordinateur.

9. Cliquez sur OK pour lancer le processus d'authentification.
11. Eteindre le MD-N32 (ou l'alimentation du panneau en cas d'utilisation du module intégré, tel que le MD-IP32), puis le rallumer. Cette étape est nécessaire lors de l'utilisation de certaines versions des modèles MD-N32 ou MD-IP32. Sautez cette étape si elle n'est pas applicable.
12. Si la configuration s'applique à un réseau WAN, déconnectez l'unité configurée du réseau local et reconnectez-vous au réseau WAN et au réseau des centrales de contrôle d'accès fonctionnant sur le WAN.

Annexe C. Configuration des compteurs d'utilisateurs

Vous pouvez utiliser les options du compteur d'utilisateurs pour limiter le nombre d'accès d'un utilisateur particulier. Pour ce faire, utilisez l'option Compteurs qui apparaît dans la fenêtre Propriétés de l'utilisateur (**User Properties)**.

Pour configurer les compteurs d'utilisateurs:

1. Sélectionnez l'onglet Général (**General)** de la fenêtre Propriétés de l'utilisateur (**User Properties)** dans le cadre de la procédure pour ajouter un nouvel utilisateur ou sélectionner un utilisateur existant.
2. Dans la barre d'outils, cliquez sur l'icône 
3. Dans la section Compteur de la fenêtre Propriétés de l'utilisateur (**User Properties)** électionnez Activer (**Enable)**.
4. Sélectionnez Définir un nouveau compteur (**Set New Counter)** t indiquez le nombre d'entrées autorisées pour l'utilisateur dans le champ Valeur du compteur (**Counter Value)**.

5. Cliquez sur **OK**.
6. Sélectionnez l'onglet Général (**General)** des propriétés du lecteur (**Reader Properties)**.
7. Dans la section Détails (Details), sélectionnez Déduire le compteur de l'utilisateur (**Deduct User counter)**.
8. Cliquez sur **OK.**

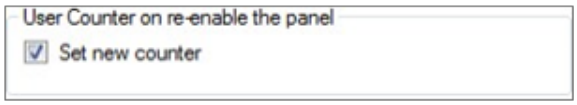
C.1 Remise à zéro du compteur lors de la réactivation du panneau

Il existe une option de compteur supplémentaire qui vous permet de réinitialiser le compteur utilisateur à sa valeur initiale dans le cas où un panneau est éteint puis rallumé.

Si cette option n'est pas utilisée, lorsque le panneau est réactivé, le compteur de l'utilisateur reprend la valeur antérieure à la désactivation du panneau.

Pour réinitialiser le compteur de l'utilisateur lors de la réactivation du panneau:

1. Dans l'arborescence, développez l'élément **AC Networks.**
3. Sélectionnez un réseau.
3. Dans la barre d'outils, cliquez sur l'icône 
4. Sélectionnez l'onglet **Options**.
5. Sélectionnez Définir un nouveau compteur (**Set new counter)**.



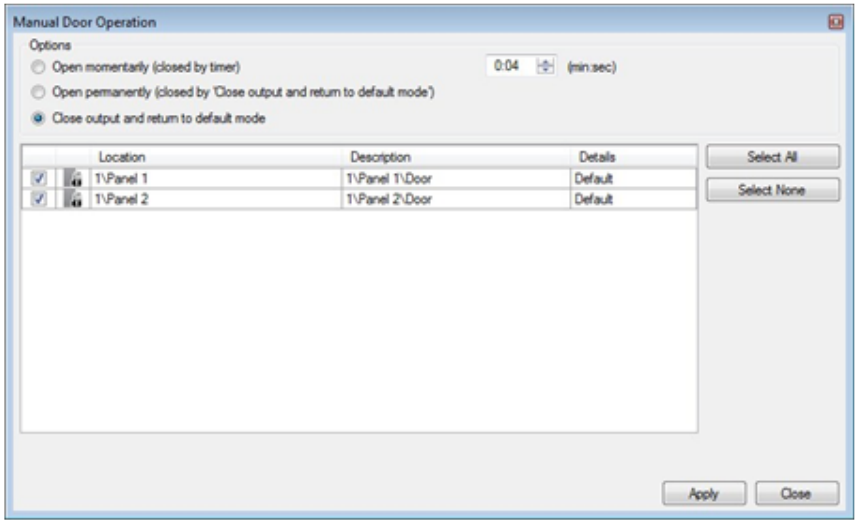
6. Cliquer sur **OK**.

Annexe D. Fonctionnement manuel de la porte

La fenêtre de fonctionnement manuel des portes (**Manual Door Operation)** permet à un opérateur d'ouvrir ou de fermer directement un groupe de portes sélectionné.

Pour ouvrir ou fermer manuellement une porte:

1. Dans l'arborescence, développez l'élément **AC Networks.**
2. Développez un réseau et développez un panneau.
3. Sélectionnez Portes (**Doors)**.
4. Dans la barre d'outils, cliquez sur l'icône 



5. Triez les panneaux/portes répertoriés dans l'ordre normal ou inverse en cliquant sur l'en-tête de colonne avec le bouton gauche de la souris.
6. Sélectionnez une option:

   Ouvrir momentanément (**Open momentarily)** - Ouvrir toutes les portes sélectionnées pendant la durée définie dans la case de la minuterie

   Ouvrir en permanence (Open permanently) – Ouvre toutes les portes sélectionnées

   Fermer la sortie (Close output) – Ferme toutes les portes sélectionnées et rend le contrôle à AxTraxPro
7. Cochez les cases des portes auxquelles l'opération doit être appliquée.
8. Cliquez sur Appliquer (**Apply)**.

Si la commande de sortie manuelle pour ouvrir une porte est désactivée, la porte peut toujours être ouverte dans une carte d'état, voir **Ouverture manuelle d'une porte à partir de la carte d'état.**

Annexe E. Enregistrement d'un visage depuis un terminal

Cette option est disponible pour les utilisateurs connectés à un terminal.

Pour enregistrer un visage via un terminal :

1. Assurez-vous que le terminal biométrique est connecté
2. Dans l'arborescence, déroulez l'élément **Utilisateurs**
3. Développez l'élément **Services/Utilisateurs** et sélectionnez le service approprié.
4. Sélectionnez l'utilisateur et cliquez sur l'icône 
5. Dans l'onglet Identifiants (**Credentials**) de la fenêtre Propriétés des utilisateurs (section de l'onglet Informations d'identification), cliquez sur Inscrire le visage à partir du terminal.

6. Sélectionnez la source d'inscription.
7. Cliquez sur Enregistrer (**Enroll)**.

   La case de gauche affiche le statut, tandis que la case de droite indique le temps qu'il vous reste pour enregistrer votre visage.

8. Placez-vous devant le terminal, attendez que votre visage soit identifié et suivez les instructions qui s'affichent à l'écran.

   Une fois le visage enregistré, un message de réussite apparaît dans la case de gauche..
9. Cliquez sur **OK**.

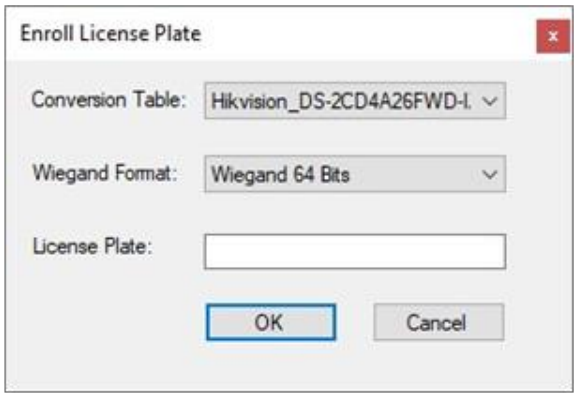
   La fenêtre se ferme et l'enregistrement du nouveau visage apparaît dans la zone **Détails.**
10. Cliquez sur **OK** dans la fenêtre **Propriétés de l'utilisateur** pour accepter les informations d'identification du visage.

Annexe F. Enregistrement d'une plaque d'immatriculation

Cette option permet de convertir les caractères alphanumériques lus par une caméra tierce en format Wiegand à l'aide d'une table de conversion définie par l'utilisateur et comprise par le système AxTraxPro.

Pour enregistrer une plaque d'immatriculation:

1. Dans l'arborescence, développez l'élément **Utilisateurs.**
2. Développez l'élément **Départements/Utilisateurs** et sélectionnez le département concerné.
3. Sélectionnez l'utilisateur et cliquez sur l'icône 
4. Dans l'onglet Identifiants (**Credentials)** de la fenêtre Propriétés de l'utilisateur (**Users Properties)** (voir Credentials Tab), Cliquer sur **Enroll from License Plate**.



5. Sélectionnez la table de conversion (voir Conversion Tables).
6. Entrez le numéro d'immatriculation du véhicule.
7. Cliquer sur **OK**.

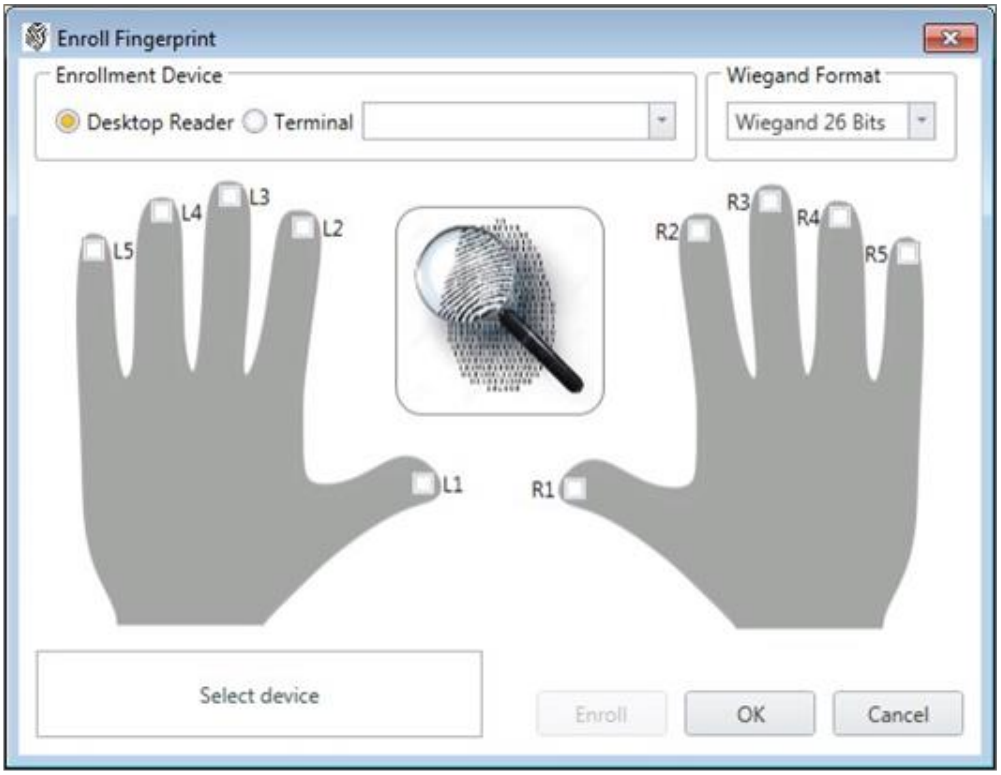
Annexe G. Enregistrement de l'empreinte digitale d'un utilisateur

Si vous utilisez le lecteur de bureau d'empreintes digitales DR-B9000, vous devez installer un pilote spécial sur votre PC Windows.

Cette option est disponible pour les utilisateurs qui doivent utiliser un terminal biométrique.

Pour enregistrer l'empreinte digitale d'un utilisateur à l'aide d'un lecteur biométrique:

1. Assurez-vous que le terminal biométrique est connecté.
2. Dans l'arborescence, développez l'élément **Utilisateurs**.
3. Développez l'élément **Départements/Utilisateurs** et sélectionnez le département concerné.
4. Sélectionnez l'utilisateur et cliquez sur l'icône 
5. Cliquez sur l'onglet Identifiants (**Credentials)** dans la fenêtre Propriétés de l'utilisateur (**Users Properties)** (voir Credentials Tab), puis cliquez sur Ajouter à partir d'un lecteur d'empreintes digitales (**Add from a Fingerprint Reader)**.

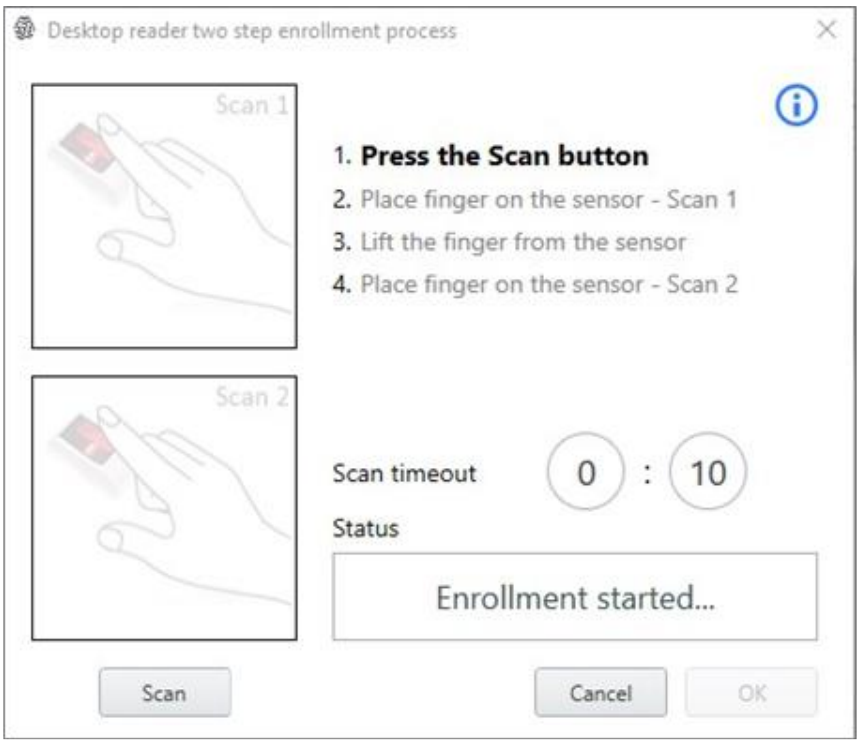


6. Sélectionnez la source d'enregistrement (Enrollment Device).

Si vous utilisez un lecteur de bureau d'empreintes digitales, vous aurez une procédure de connexion en deux étapes en plus d'une image d'empreintes digitales en direct.

7. Sélectionnez le doigt que vous souhaitez enregistrer.

10. Cliquez sur **Enroll.** Vous devriez voir l'écran ci-dessous. Suivez les instructions à l'écran pour réussir l'enregistrement..

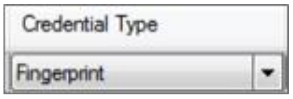


9. Appuyez sur le **bouton de scannage**.
10. Placez le doigt sur le capteur - Scan 1.
11. Retirez le doigt du capteur. Attendez 3 secondes
12. Placez le doigt sur le capteur - Scan 2

    Vous devriez voir que le doigt a été lu avec succès, comme indiqué ci-dessous.

13. Cliquez sur **OK.**

    La fenêtre se ferme et la nouvelle empreinte digitale apparaît dans la zone **Détails.**



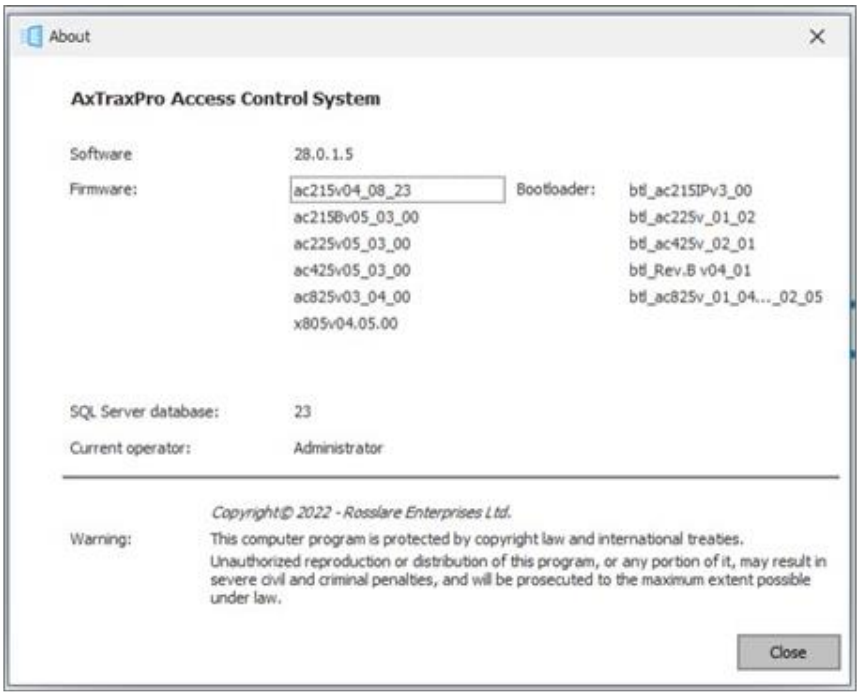
14. Cliquez sur **OK** dans la fenêtre **Propriétés de l'utilisateur** pour accepter l'empreinte digitale.

Annexe H. Menu Aide

Le menu Aide comporte quatre options:

H.1 À propos de

La fenêtre **À propos de** affiche les versions du logiciel, du micrologiciel et de la base de données, ainsi que les informations relatives à l'opérateur actuel et à la licence.



H.2 Manuel de l'utilisateur

En cliquant sur le **Manuel de l'utilisateur**, le manuel de l'utilisateur d'AxTraxPro s'ouvre..

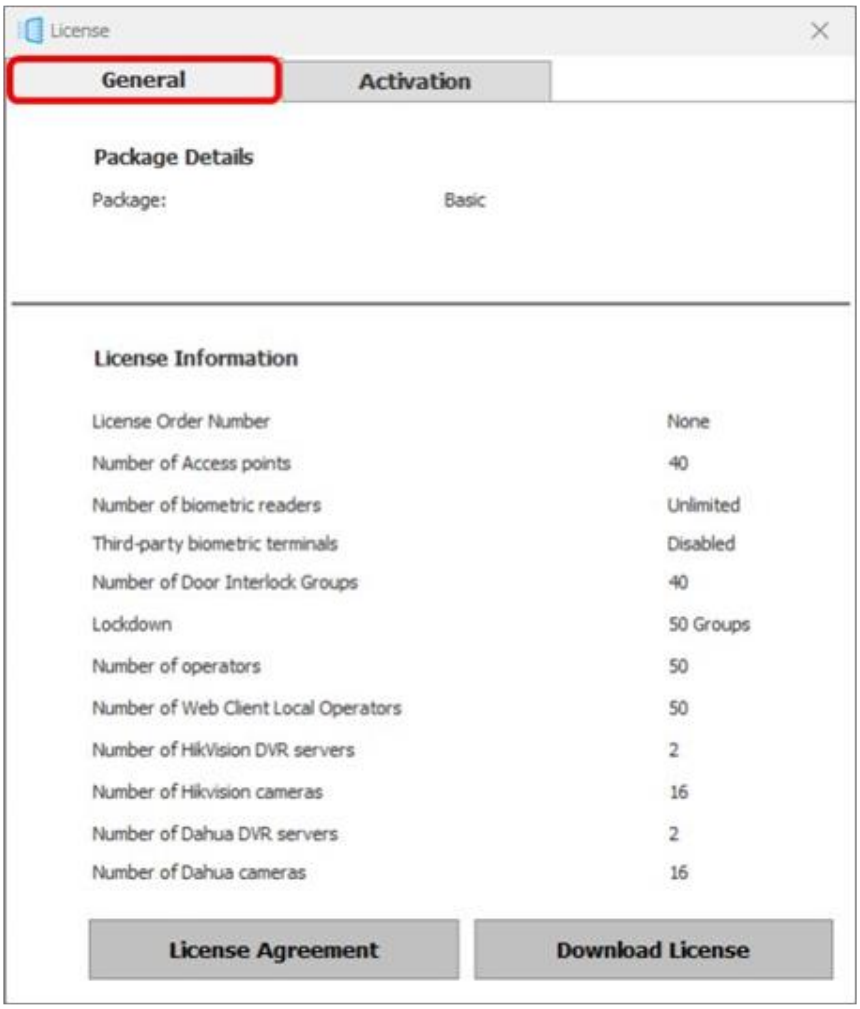
H.3 Activation du code produit AxTraxPro

La fenêtre Licence permet d'obtenir des informations sur la licence en cours et d'activer une nouvelle licence.

H.3.1 Informations générales sur AxTraxPro et sur le contrat de licence

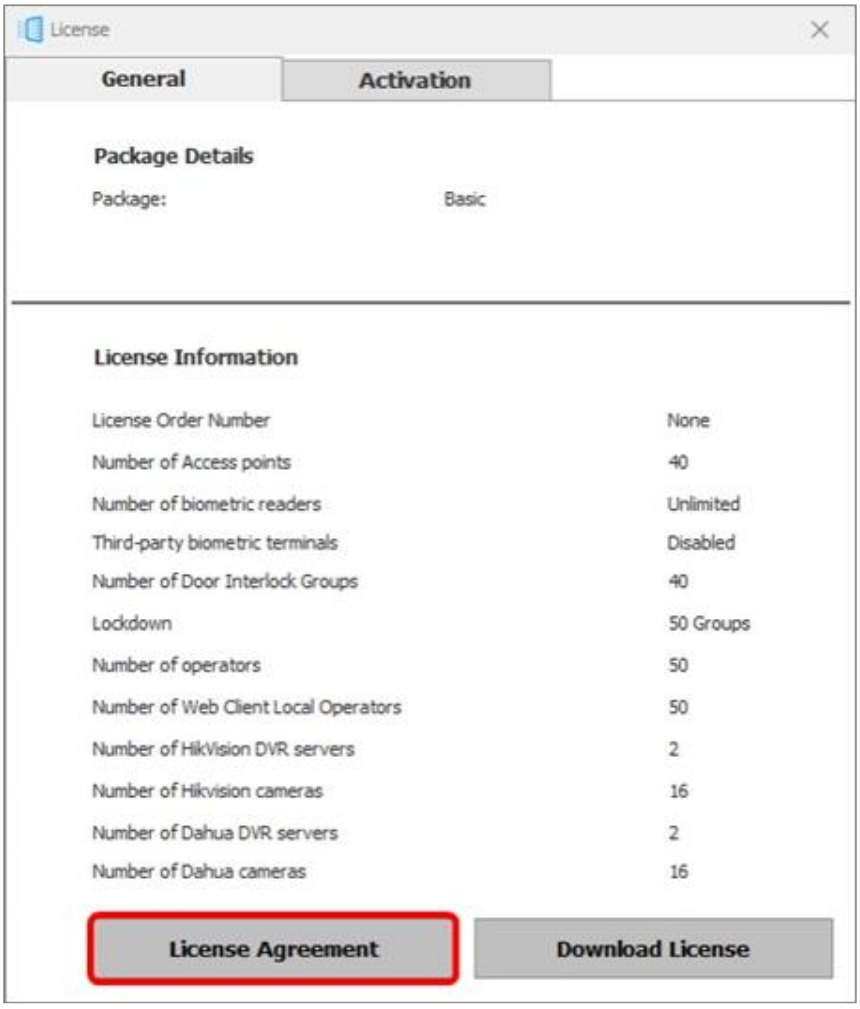
Pour lire les détails du plan:

1. Dans la barre de menu, sélectionnez **Help > License**.
2. Cliquez sur l'onglet **General**.



Pour lire l'accord de licence:

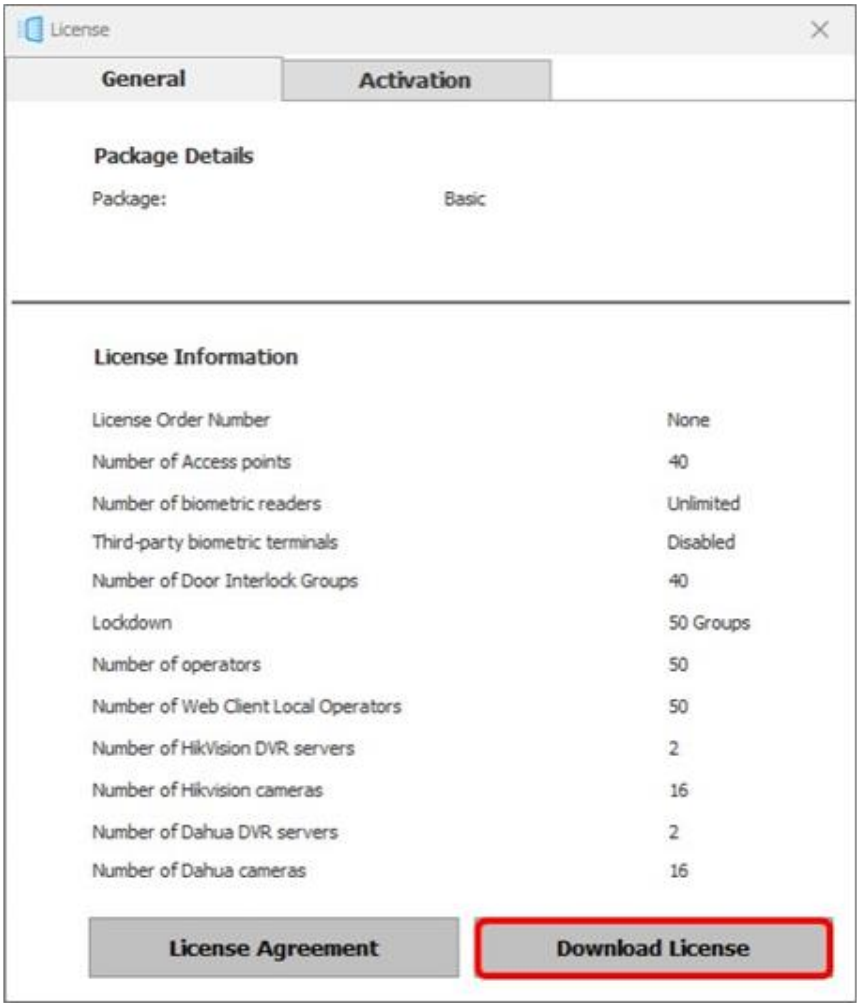
1. Dans la fenêtre de l'onglet Général (**General),** cliquez sur **License Agreement**



L'accord de licence (**License Agreement)** s'affiche dans une fenêtre contextuelle.

Pour télécharger la licence actuellement activée:

1. Dans la fenêtre de l'onglet Général (**General),** cliquez sur **Download License**.



2. Recherchez un emplacement pour enregistrer le fichier.
3. Cliquez sur **Save**.

H.3.2 Activation du client AxTraxPro Desktop

Pour activer AxTraxPro sur un PC, il est nécessaire de fournir une clé de licence. La procédure d'activation est décrite ci-dessous.

Après l'installation, une licence **Basic Plan** est intégrée au logiciel.

Téléchargez et envoyez le Hardware ID à Rosslare:

1. Dans la barre de menu, sélectionnez **Help > License**.
2. Cliquez sur l'onglet **Activation**.

L'ID du matériel est rempli automatiquement..

3. Cliquer sur **Download**.
4. Naviguez jusqu'à l'emplacement où vous souhaitez enregistrer le fichier.

Enregistrez le fichier (xxx.license) sur votre PC à un endroit facilement accessible.

5. Cliquer sur **Save**.
6. Envoyez **l'ID du matériel** à Rosslare en demandant un fichier de clé de licence (**License Key File).**

Activer Rosslare sur un PC:

1. Décompressez le fichier de clé de licence (**License Key File)** que vous avez reçu de Rosslare.
2. Sauvegardez le fichier (xxx.license) sur votre PC à un endroit facilement accessible.

4. Cliquer sur ... pour localiser le fichier de la clé de licence (**License Key File**).
4. Double-cliquez sur le fichier de clé de licence (**License Key File)**.
5. Cliquer sur **Activate**.

H.4 Feedback

Utilisez le formulaire de la fenêtre Feedback pour envoyer un feedback à Rosslare.

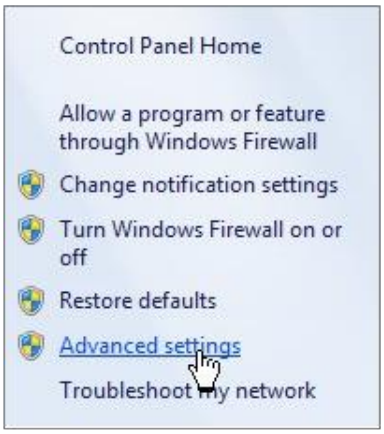
Pour utiliser le formulaire de feedback, configurez les paramètres SMTP (voir Paramètres de notification (Notification Settings).

Annexe I. Ouverture d'un programme dans le pare-feu Windows

Pour ouvrir un port dans le pare-feu de Windows:

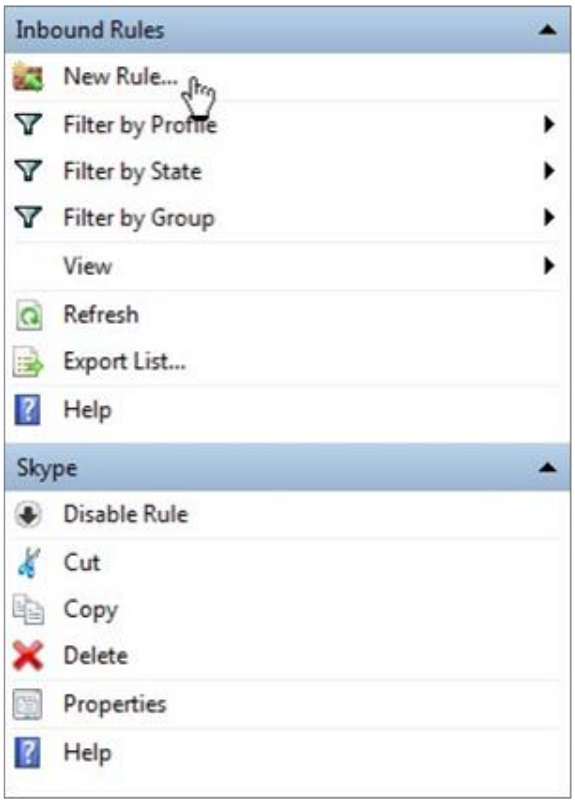
1. Ouvrez le panneau de configuration.
2. Cliquez sur la catégorie Pare-feu Windows (**Windows Firewall)**.

3. Cliquez sur **Paramètres avancés** dans la colonne de gauche de la fenêtre Pare-feu Windows.



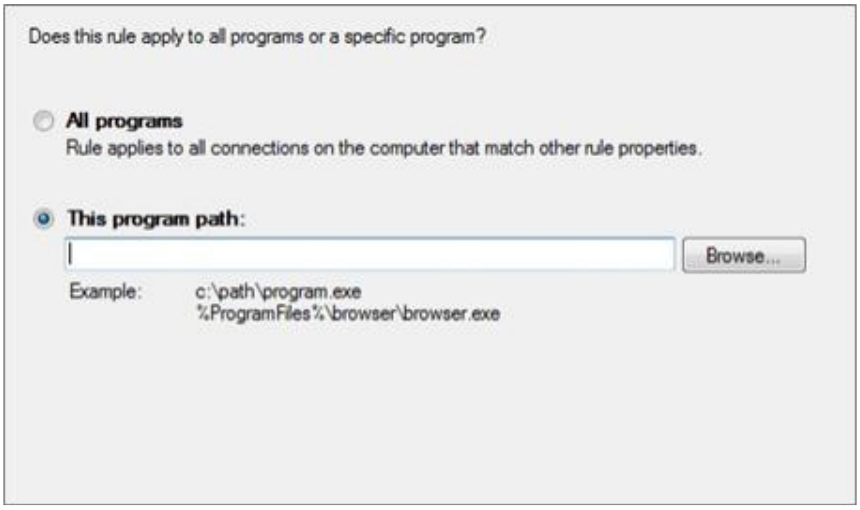
4. Dans l'arborescence de la console à gauche, cliquez sur **Inbound Rules**.

5. Dans la colonne de droite, cliquez sur **New Rule**.



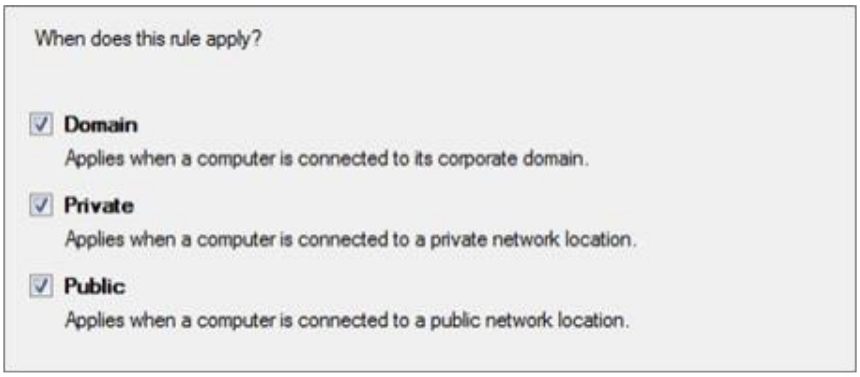
6. Assurez-vous que l'option "**Program**" est sélectionnée.

7. Cliquer sur **Next**



8. Assurez-vous que "Ce chemin de programme" (**This program path)** est sélectionné.
9. Cliquez sur "Parcourir" (**Browse)** et localisez le fichier AxtraxServerService.exe, qui se trouve dans *C:\Program Files (x86)\Rosslare\AxTraxPro Server*.
10. Cliquer sur **Next**.

11. Assurez-vous que l'option "Autoriser la connexion" (**Allow the connection)** est sélectionnée.
12. Cliquer sur **Next**.



13. Assurez-vous que les trois cases sont cochées.
14. Cliquer sur **Next**.

15. Entrez un nom pour la règle, par exemple "Pro Server", et cliquez sur Terminer (**Finish)**.

Annexe J. Problèmes de connexions WAN

Cette annexe présente trois scénarios de problèmes de connexion au serveur.

J.1 Le serveur est en panne ou la configuration de l'IP et du port est erronée

Au démarrage du client AxTraxPro, le message d'erreur suivant apparaît.

Cliquer sur **OK** pour fermer le client AxTraxPro et démarrer l'outil de configuration AxTraxPro.

J.2 Arrêt du serveur ou erreur réseau entre le client AxTraxPro et le serveur AxTraxPro

Le journal des événements indique une erreur de communication:

Vérifiez si le serveur est en panne. Vérifiez si l'adresse a changé ou si la connexion réseau présente des erreurs.

J.3 Les paramètres IP+Port sont corrects mais le client ne démarre pas

Vérifiez les problèmes de pare-feu suivants:

- Vérifier le pare-feu du PC serveur
- Vérifier le pare-feu du PC client
- Vérifier le pare-feu du réseau du serveur
- Vérifier le pare-feu du réseau du client

Pour plus d'informations sur l'assistance, veuillez consulter le site https://support.rosslaresecurity.com.

5 0 + 9 0 7 0 6 9 0 - 6 0 7 0